Version

0.1.8

3SP LTD

SSL and SSH-Based Security Solutions

SSL-Explorer Reference Guide

3SP LTD

SSL-Explorer

No. 3 • Glade Business Centre • Forum Road • Nottingham • United Kingdom
Phone +44 (0) 115 951 9692 • Fax +44 (0) 115 951 9652

Table of Contents

Chapter

1

An Introduction to SSL-Explorer

So what's this SSL VPN stuff all about anyway? What can it do for me and my company?

The SSL-Explorer VPN from 3SP Ltd is the world's first open source Java-based SSL VPN solution.

Corporate VPNs have become a hot topic in recent years, and none more so than SSL-based varieties. The benefits to productivity and the low maintenance overhead that comes with browser-based connectivity is something that cannot be dismissed by most businesses, though the costs of implementation can often be prohibitive.

The advantage of using Secure Sockets Layer lies primarily in the fact that all standard web browsers support this mode of communication by default. This stands in direct contrast to existing IPSec VPNs, where client-side code needs installing on each connecting PC, thereby raising the management overhead and implementation costs associated with said solutions.

Consider that in many situations these days; installing client VPN software is simply not possible due to administrative software installation policies and firewall rules. Using IPSec from an Internet café to quickly retrieve a file you left in the office is simply unworkable.

Another prime advantage of SSL-based VPNs is that by design, they operate at the application layer. Essentially, this means that they are not subject to any form of network traversal issues or to strict firewall policies – if you are able to access your internet banking website from your chosen location, then you can most likely also use SSL-Explorer.

Of course, SSL-Explorer goes much further than just the basics. By leveraging the trusted, secure architecture provided by the industry standard SSL protocol, a series of additional services are offered to provide file access to Microsoft Windows networks, either through its web browser interface, or with full integration into your Windows Explorer filesystem browser.

Access to internal intranet resources is also a breeze with SSL-Explorer. As a network administrator, you can simply publish links to say, your web-based CRM system, or maybe your software issue tracker. You can forget about helpdesk enquiries from remote users; it doesn't get much easier than clicking on a link.

Active Directory integration allows you to use your existing Microsoft Windows user and group hierarchies to assign access rights. Users can easily be set up to authenticate with SSL-Explorer using their Windows domain credentials – they won't need to write down yet another password on their monitors.

For software developers, there's a defined Application Programming Interface (API) that can be used to leverage the features provided by the VPN client in your applications. This has already been done in a popular CVS client named SmartCVS[1] to provide remote access to internal software repositories by using the SSL-Explorer to both proxy and encrypt source code.

You can deploy Java-based applications to your users on the VPN. To take a real world example, this means that you can publish the Citrix client on SSL-Explorer and enjoy secure Citrix sessions. For the administrator, we'll soon be making available a series of lightweight client applets to allow for fully integrated SSH, VNC, SFTP access to manage your network infrastructure remotely. Or in the meantime, use these features right now in our client application, SSHTerm Professional.

So as you can see, the SSL-Explorer solution is already almost fully-featured even before its 1.0 release. Though quite possibly the main selling point – and probably the reason you're even reading this – is that all these features (and more to come) are totally free to use. This software is licensed under the Gnu General Public License (GPL) which allows use of the software in a commercial, or non-commercial environment without payment of licensing fees.

Our intention with SSL-Explorer is to bring enterprise-class features to smaller businesses or individuals with a heavy requirement for remote access to their resources. It's these users that maybe can't justify the costs involved to implement market leading solutions in their smaller environments, and it's also these users that many vendors tend to overlook in their desire to secure larger and more profitable customers.

All of us here at 3SP Ltd hope you enjoy the application!

[1] SmartCVS – http://www.smartcvs.com

Chapter

2

Before You Begin…

Don't jump in head first. Check here to make sure you have the necessary kit before you begin.

Hardware Requirements

You will require some hardware to install SSL-Explorer. We're assuming that you intend to install SSL-Explorer on a standalone PC inside your office network with external connections to port 443 forwarded by your firewall to SSL-Explorer.

- Pentium III 1Ghz CPU or greater (will install on lesser machines but will be less responsive)
- 512MB RAM recommended
- 150 MB free hard disk space
- Internet connection

Performance Considerations

Depending upon your exact requirements, the SSL-Explorer server will be serving web pages, encrypting data in real time and establishing many performance intensive HTTPS transactions – potentially between many concurrent users. If you intend on providing remote access to many users simultaneously then do expect to invest a reasonable amount in a high-specification system to achieve good results. For a smaller company (5-10 users), the hardware requirements listed above should be fine.

Other Operating Systems

If your operating system is not listed, you may want to try compiling the software from source on your OS?

How many other VPN vendors let you do that?

Please let us know of the outcome so we can extend our officially supported operating systems list!

Operating System Requirements

The SSL-Explorer server was written in the Java programming language to ensure that it can run on any operating system with a Java 5.0 runtime environment.

Unfortunately this does mean that the software will not install on the Apple MacOSx platform as Java 5.0 will not be released for this platform until the future release of Tiger 10.4.

In the meantime, we are investigating options for reducing the Java platform requirement to 1.4.2.

The officially supported operating systems at the time of writing are:

- Microsoft Windows 2000/XP/2003
- Red Hat Linux 8.0 or later

There are installation packages available for these operating systems in Windows executable format and Linux RPM format.

For Windows, please use:
💾 ssl_explorer_windows_0_x_x.exe

For Linux, please use:
💾 ssl_explorer_linux_0_x_x.rpm

Check before you install

All SSL-Explorer software is published through the SourceForge community website at http://sourceforge.net/projects/ssl-explorer. Please do not install SSL-Explorer software downloaded from anywhere else as we cannot guarantee the authenticity of software obtained through third party download sites. As the source code is freely published, you should always ensure that you trust the authenticity of your downloaded software.

Chapter 3

Installation of SSL-Explorer

Let's walk through the installation of SSL-Explorer on today's mainstream operating systems.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Keyboard exercise
- 🕮 Workbook review

SSL-Explorer on Microsoft Windows

In this walkthrough, we will take you through the installation of SSL-Explorer on the Microsoft Windows operating system. The operating system used is Windows XP with Service Pack 2 installed.

A clean installation of your chosen Windows operating system and application of all published service packs and/or hot-fixes is recommended.

It is not prudent to consider installing a security solution onto a Windows system without first ensuring that the system is firstly up-to-date with all published service packs and hot-fixes.

SSL-Explorer requires Java Runtime Environment (JRE) 5.0 to operate. The JRE is the software that allows your computer to understand applications written in Java. Don't worry if you haven't installed it, or don't know where to get it from because the installer will take care of that for you.

Once you have downloaded the software onto your chosen machine, you may begin.

🗀 SSL-Explorer and the Windows XP SP2 Firewall

We have noticed that when installing the SSL-Explorer VPN server on a Windows XP SP2 machine with firewall enabled, the Web based filesystem browser fails to start in some cases. We're currently looking into this issue although we recommend in all cases that your SSL-Explorer server should not be both firewall and VPN server. If you encounter problems, please check whether the problem disappears when the firewall is disabled before contacting the help forums.

Windows Installation Process

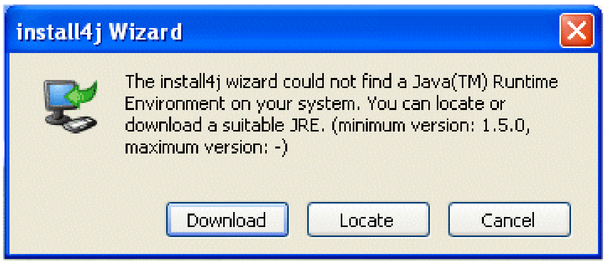
Firstly remove old versions of SSL-Explorer

As of release 0.1.8 there is no upgrade capability for your SSL-Explorer database. This means that settings cannot yet be preserved between new installations. **Make sure you uninstall older versions and manually delete all files left under the original installation directory before attempting to install a new version.**

1. Double-click the SSL-Explorer installation file, named similarly to below, where 'x' denotes the current release.

   ssl_explorer_1_x_x.exe

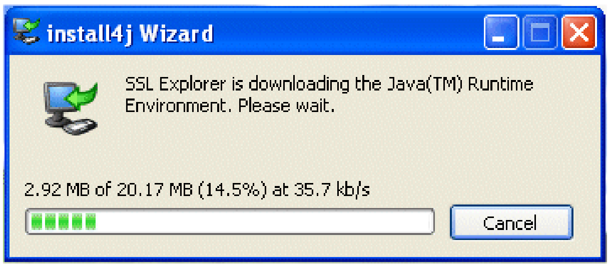
2. The installation process will begin and will attempt to locate a copy of the Java 5.0 JRE. You will see a dialog similar to the one below if it was unsuccessful.



The install4j wizard could not find a Java(TM) Runtime Environment on your system. You can locate or download a suitable JRE. (minimum version: 1.5.0, maximum version: -)

3. Click download to start an automatic download and installation of the Java 5.0 JRE.

   Note: If you use a proxy server to access the internet, you may need to download the Java 5.0 JRE manually[2]. The installer uses Internet Explorer's connection settings to determine proxy status.

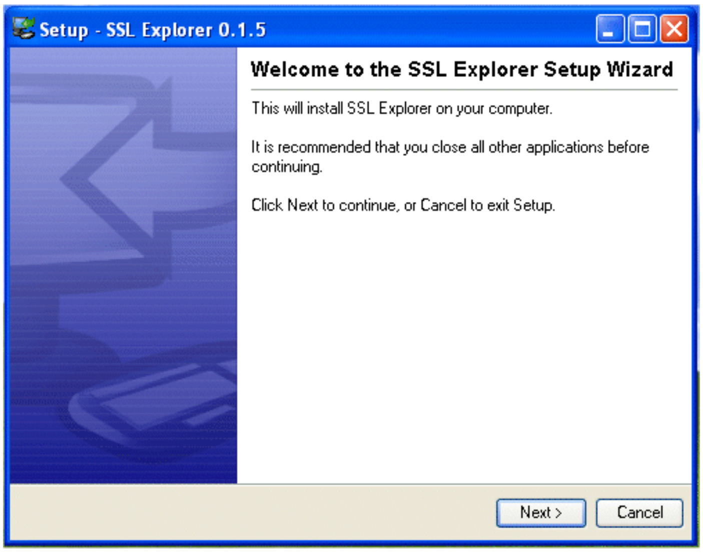


SSL Explorer is downloading the Java(TM) Runtime Environment. Please wait.

2.92 MB of 20.17 MB (14.5%) at 35.7 kb/s

[2] The Sun Microsystems Java 5.0 JRE for Windows can be found at: http://java.sun.com/j2se/1.5.0/download.jsp

4. Once the JRE has been downloaded and installed, you will be presented with the SSL-Explorer installation dialog. Click next to begin the installation.



Setup - SSL Explorer 0.1.5

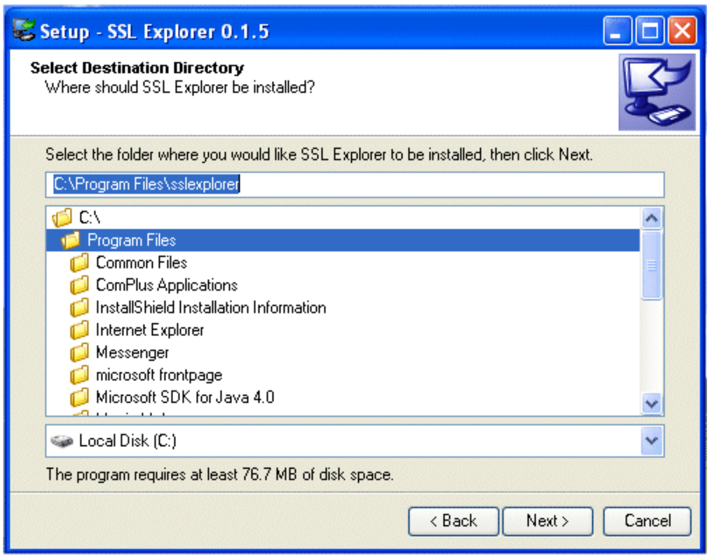
Welcome to the SSL Explorer Setup Wizard

This will install SSL Explorer on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

5. Firstly, choose a location to install the SSL-Explorer files. Accepting the suggested location should not cause any problems.



Setup - SSL Explorer 0.1.5

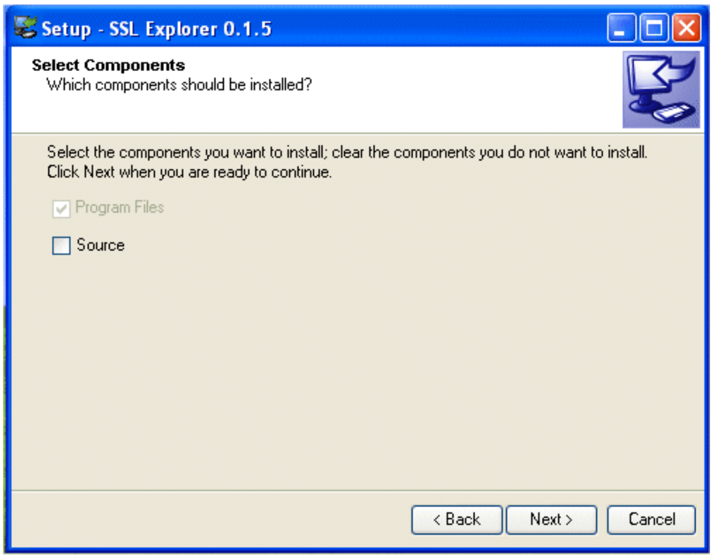
Select Destination Directory
Where should SSL Explorer be installed?

Select the folder where you would like SSL Explorer to be installed, then click Next.

C:\Program Files\sslexplorer

The program requires at least 76.7 MB of disk space.

6. The installer will now ask you whether you want to install the source code for the SSL-Explorer software. You do not have to install the source code in order to use SSL-Explorer. This option is provided for advanced users and will install the Java source files that were used to develop the application.



Setup - SSL Explorer 0.1.5

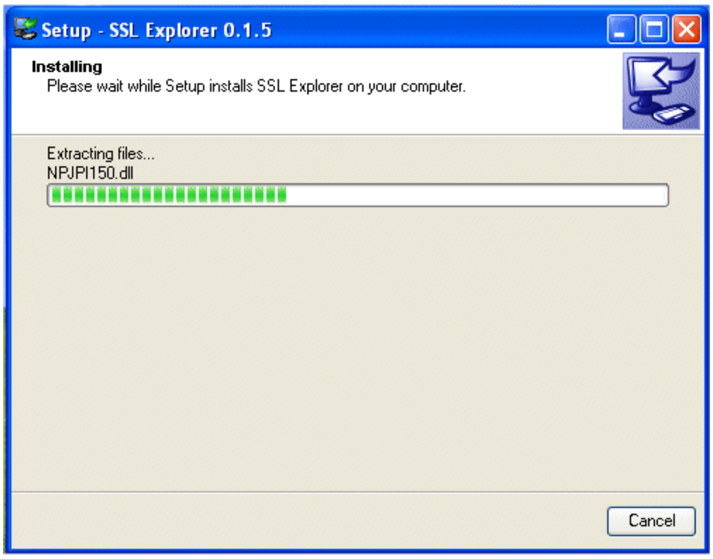
Select Components
Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☑ Program Files

□ Source

7. The installer has now collected all the information it needs to begin. Click next to start the program installation and the SSL-Explorer program files will be installed to your chosen directory.

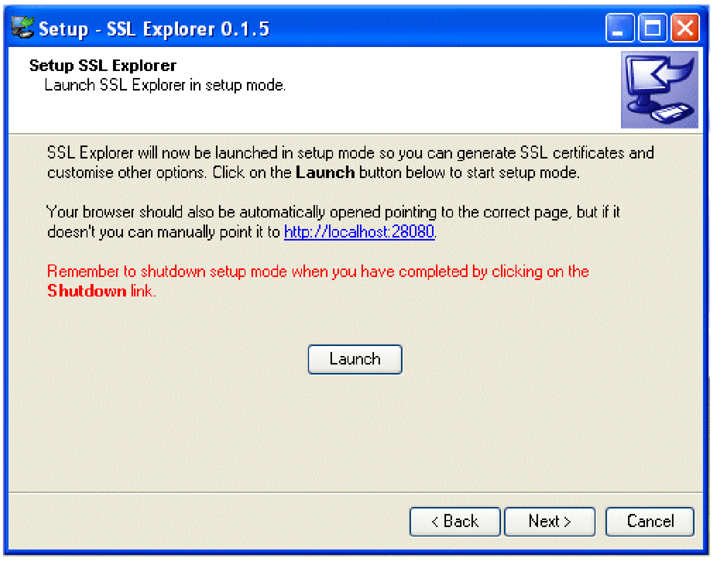


Setup - SSL Explorer 0.1.5

Installing
Please wait while Setup installs SSL Explorer on your computer.

Extracting files...
NPJPI150.dll

8. Once the program files have been successfully copied, the installer will prompt you to connect to your server in setup mode. Click the launch button to start the SSL-Explorer service and open a web browser that will connect to your server's configuration utility.



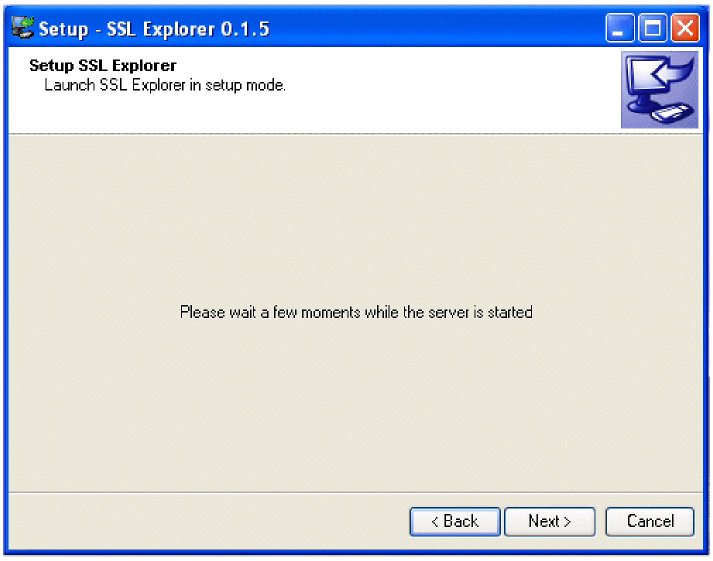
Setup SSL Explorer
Launch SSL Explorer in setup mode.

SSL Explorer will now be launched in setup mode so you can generate SSL certificates and customise other options. Click on the **Launch** button below to start setup mode.

Your browser should also be automatically opened pointing to the correct page, but if it doesn't you can manually point it to http://localhost:28080.

Remember to shutdown setup mode when you have completed by clicking on the **Shutdown** link.

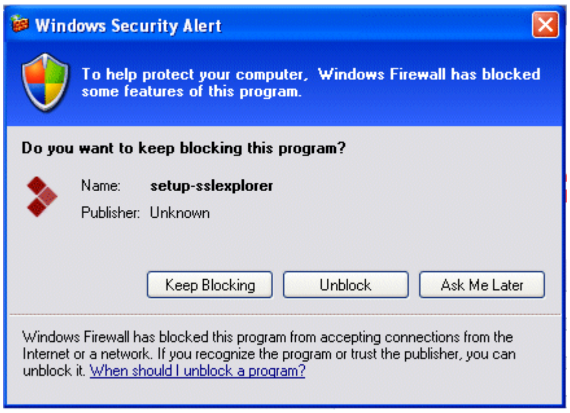
9. The service is started.



Setup SSL Explorer
Launch SSL Explorer in setup mode.

Please wait a few moments while the server is started

10. Click next. If you are installing the SSL-Explorer on a Microsoft Windows system that has Service Pack 2 installed, the following dialog will appear. This is the Windows firewall that detects that the SSL-Explorer setup utility is trying to access your network and will prompt you to take action. Choose "Unblock" to allow network access for the SSL-Explorer configuration utility.



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: setup-sslexplorer

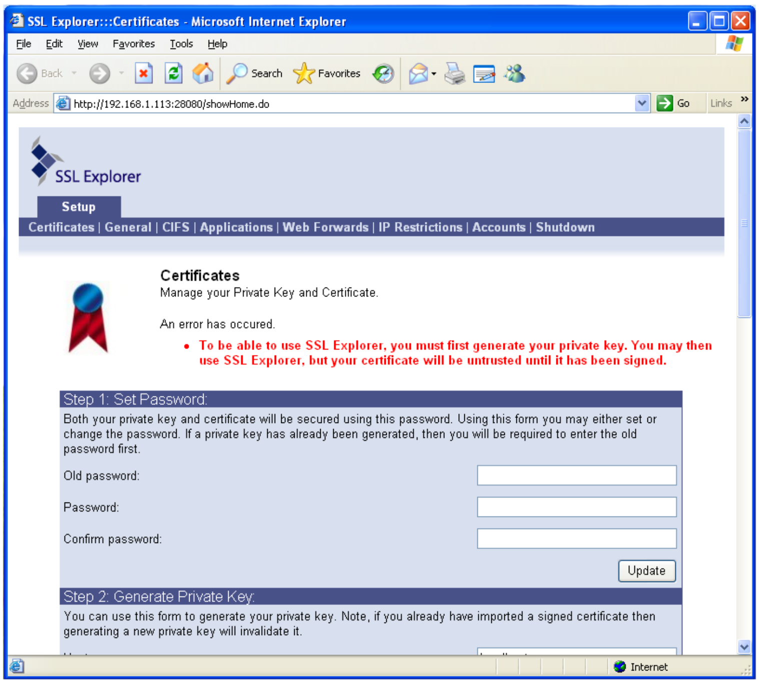
Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

SSL Certificates

It is recommended that you purchase a certificate from a CA for use with SSL-Explorer. The import of third party SSL certificates is covered later.

11. Your web browser should have connected to your SSL-Explorer server. The first screen you will see is the SSL certificate management page.



SSL Explorer:::Certificates - Microsoft Internet Explorer

Address: http://192.168.1.113:28080/showHome.do

Certificates

Manage your Private Key and Certificate.

An error has occured.

- To be able to use SSL Explorer, you must first generate your private key. You may then use SSL Explorer, but your certificate will be untrusted until it has been signed.

Step 1: Set Password:

Both your private key and certificate will be secured using this password. Using this form you may either set or change the password. If a private key has already been generated, then you will be required to enter the old password first.

Old password:

Password:

Confirm password:

Step 2: Generate Private Key:

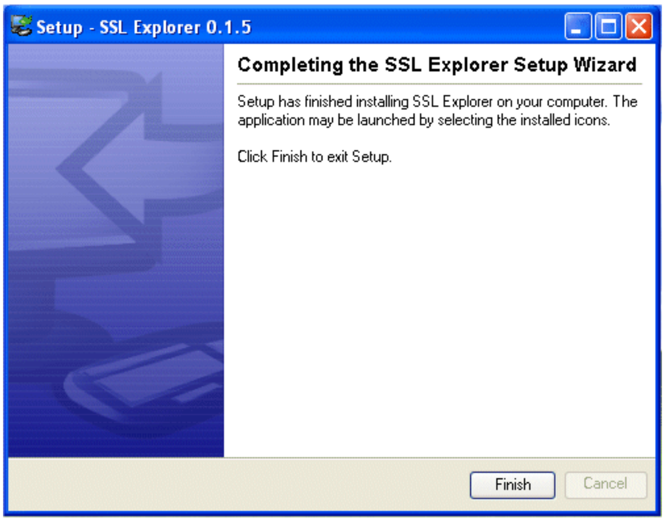
You can use this form to generate your private key. Note, if you already have imported a signed certificate then generating a new private key will invalidate it.

File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Go
Links
SSL Explorer
Setup
Certificates | General | CIFS | Applications | Web Forwards | IP Restrictions | Accounts | Shutdown
Update
Internet

12. Please now refer to the section titled **"The Web Based Setup Procedure"** to guide you through configuring your SSL-Explorer server.

13. The configuration step is now complete. Click the shutdown option to stop the SSL-Explorer service and close the browser. The setup wizard will inform you that setup is now complete.

    Click finish to close the installation program.



Setup - SSL Explorer 0.1.5

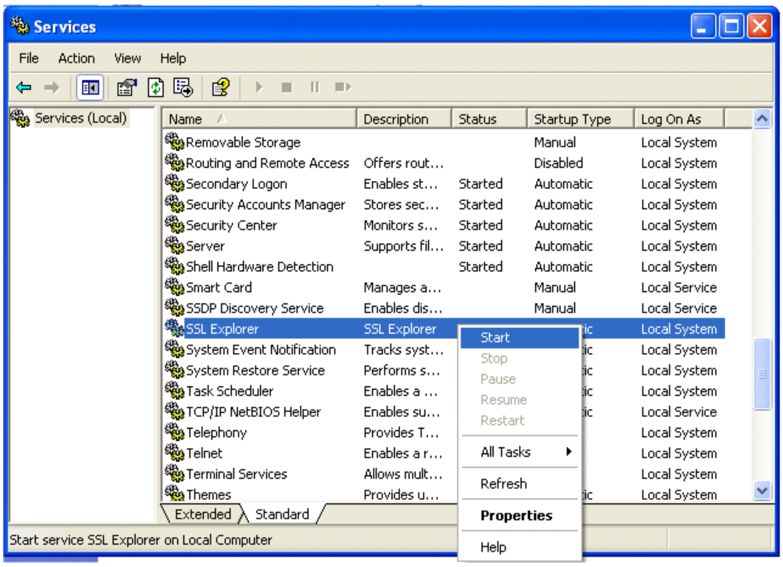
Completing the SSL Explorer Setup Wizard

Setup has finished installing SSL Explorer on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

14. Check the status of the SSL-Explorer service in **Control Panel ➔ Administrative Tools ➔ Services.**

    If the service is stopped, please start it.



Name	Description	Status	Startup Type	Log On As
Removable Storage			Manual	Local System
Routing and Remote Access	Offers rout…		Disabled	Local System
Secondary Logon	Enables st…	Started	Automatic	Local System
Security Accounts Manager	Stores sec…	Started	Automatic	Local System
Security Center	Monitors s…	Started	Automatic	Local System
Server	Supports fil…	Started	Automatic	Local System
Shell Hardware Detection		Started	Automatic	Local System
Smart Card	Manages a…		Manual	Local Service
SSDP Discovery Service	Enables dis…		Manual	Local Service
SSL Explorer	SSL Explorer		ic	Local System
System Event Notification	Tracks syst…		ic	Local System
System Restore Service	Performs s…		ic	Local System
Task Scheduler	Enables a …		ic	Local System
TCP/IP NetBIOS Helper	Enables su…		ic	Local Service
Telephony	Provides T…			Local System
Telnet	Enables a r…			Local System
Terminal Services	Allows mult…			Local System
Themes	Provides u…		ic	Local System

Start service SSL Explorer on Local Computer

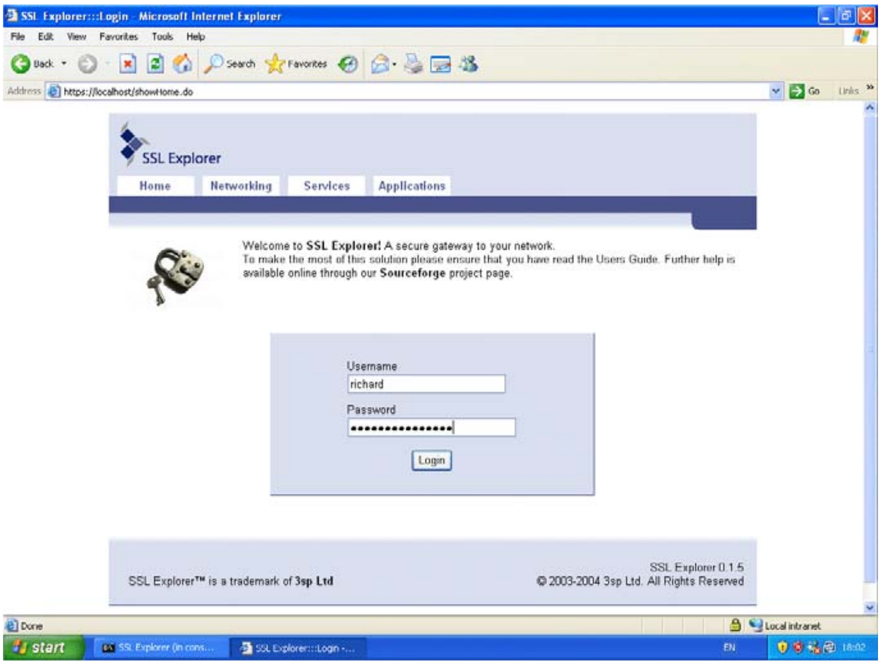
SSL-Explorer and the 1067 Service Error

If you are experiencing this error, it is most likely that IIS is running and is using port 443. You'll need to stop/disable IIS for the SSL-Explorer service to start.

15. **The installation of SSL-Explorer is now complete!** Try connecting to your server using the following URL, changing "hostname" to the hostname of the system that you installed the server on:

    https://hostname/

    You should be presented with the SSL-Explorer log on screen, similar to the following. You should now be able to log in to the system using your Active Directory credentials.



https://localhost/showHome.do

Welcome to **SSL Explorer!** A secure gateway to your network.
To make the most of this solution please ensure that you have read the Users Guide. Further help is available online through our **Sourceforge** project page.

Username
richard

Password
••••••••••••••••

SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved

Installation of SSL-Explorer on Red Hat 8.0

This guide takes you through the installation process on Red Hat Linux version 8.0. You will need to download the Java 5.0 JRE[3] from Sun Microsystems before you begin.

We are assuming that you are using the SSL-Explorer RPM package.

1. Download the Java 5.0 JRE and follow the instructions for installation.

2. Change directory to the location of your SSL-Explorer RPM package.

3. Install the SSL-Explorer either by double-clicking on its icon using the Nautilus file browser, or by executing the following command:

   ```
   rpm -i ssl_explorer_1_x_x.rpm
   ```

4. The SSL-Explorer will now have been installed to "/opt/sslexplorer". Change to this directory in your terminal.

5. If you would like SSL-Explorer to be configured as a Red Hat service, execute the following command:

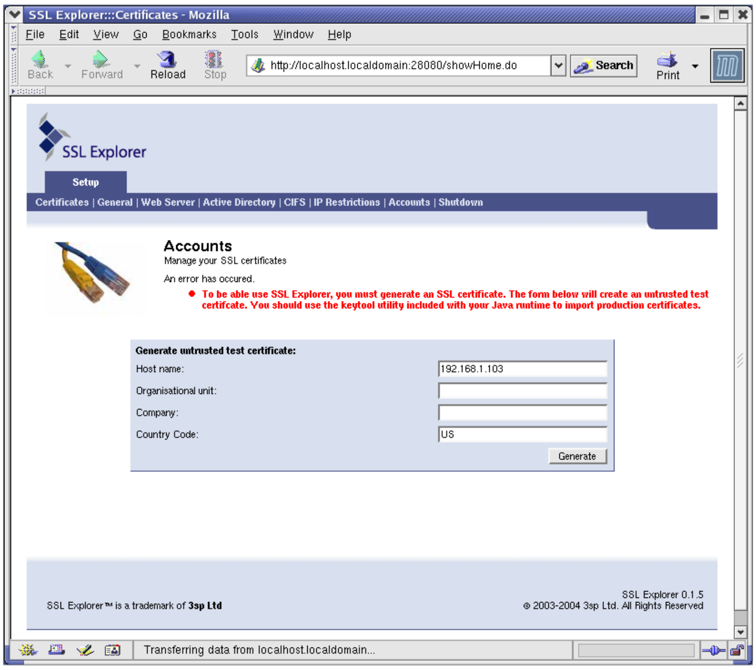
   ```
   /opt/sslexplorer/platforms/linux/install-
   service
   ```

6. Run the SSL-Explorer configuration utility as follows:

   ```
   ./setup-sslexplorer
   ```

7. The SSL-Explorer configuration utility will give you a URL which you will need to enter into your browser to begin the Web-based setup procedure. Enter the URL in your browser and you should see the following screen:

[3] The Sun Microsystems Java 5.0 JRE for Linux can be found at: http://java.sun.com/j2se/1.5.0/download.jsp


SSL Explorer:::Certificates - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:28080/showHome.do
Search
Print
SSL Explorer
Setup
Certificates | General | Web Server | Active Directory | CIFS | IP Restrictions | Accounts | Shutdown

Accounts

Manage your SSL certificates

An error has occured.

- To be able use SSL Explorer, you must generate an SSL certificate. The form below will create an untrusted test certifcate. You should use the keytool utility included with your Java runtime to import production certificates.

Generate untrusted test certificate:

Host name:	192.168.1.103
Organisational unit:	
Company:	
Country Code:	US

Generate

SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved

Transferring data from localhost.localdomain...

8. Please now refer to the next section titled **“The Web Based Setup Procedure”** to guide you through configuring your SSL-Explorer server.

9. Once you have configured SSL-Explorer to your preferences you are now ready to start the SSL-Explorer server. You can do this in one of two ways:

    a. If you installed SSL-Explorer as a service, type:

    ```
    service sslexplorer start
    ```

    b. Otherwise, run the SSL-Explorer in console mode:

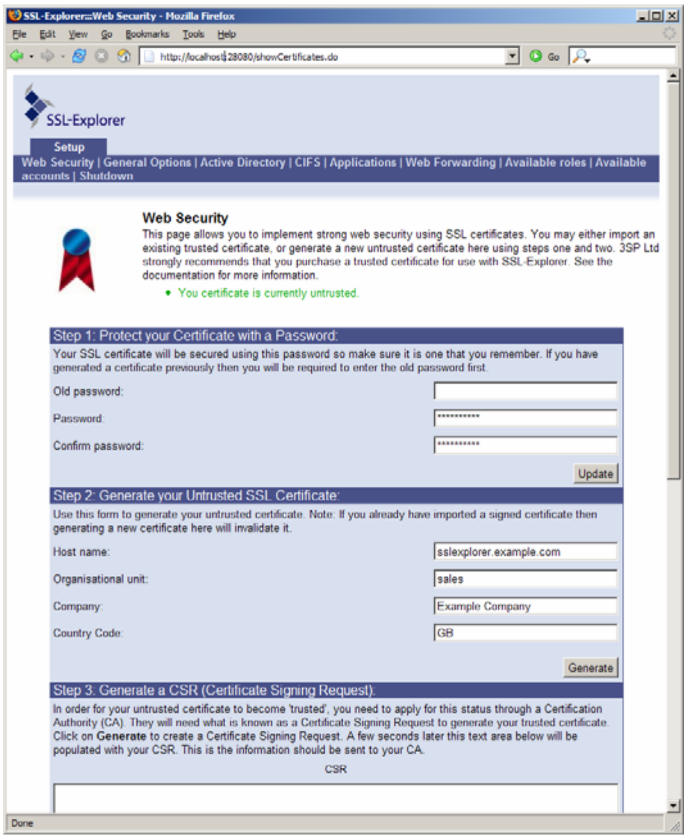
    ```
    ./sslexplorer-console
    ```

The Web-Based Setup Procedure

To ensure that installation across the various supported platforms is as consistent as possible, we have moved the majority of the post-installation configuration to a web-based setup procedure. This means no manual editing of scripts!

Please follow this procedure:

1. Your web browser should have connected to your SSL-Explorer server. The first screen you will see is the SSL certificate management page. This page will guide you through four stages that are used to configure web security features on your SSL-Explorer server.


SSL-Explorer::Web Security - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:28080/showCertificates.do
Go
SSL-Explorer
Setup
Web Security | General Options | Active Directory | CIFS | Applications | Web Forwarding | Available roles | Available accounts | Shutdown
Done

Web Security

This page allows you to implement strong web security using SSL certificates. You may either import an existing trusted certificate, or generate a new untrusted certificate here using steps one and two. 3SP Ltd strongly recommends that you purchase a trusted certificate for use with SSL-Explorer. See the documentation for more information.

- You certificate is currently untrusted.

Step 1: Protect your Certificate with a Password:

Your SSL certificate will be secured using this password so make sure it is one that you remember. If you have generated a certificate previously then you will be required to enter the old password first.

Old password:

Password: **********

Confirm password: **********

Update

Step 2: Generate your Untrusted SSL Certificate:

Use this form to generate your untrusted certificate. Note: If you already have imported a signed certificate then generating a new certificate here will invalidate it.

Host name: sslexplorer.example.com

Organisational unit: sales

Company: Example Company

Country Code: GB

Generate

Step 3: Generate a CSR (Certificate Signing Request):

In order for your untrusted certificate to become 'trusted', you need to apply for this status through a Certification Authority (CA). They will need what is known as a Certificate Signing Request to generate your trusted certificate. Click on **Generate** to create a Certificate Signing Request. A few seconds later this text area below will be populated with your CSR. This is the information should be sent to your CA.

CSR

In order to transmit data to and from the SSL-Explorer securely; you will need to generate an SSL certificate. SSL certificates are used on the internet to verify the identity of a web server in order to facilitate secure exchange of sensitive data such as credit card payments or online banking transactions.

This screen will allow you to set up an untrusted certificate in order to conduct secure SSL-Explorer sessions, or alternatively you can also import trusted certificates that have been issued by your certification authority (CA) here.

If you have not purchased a trusted certificate from a CA, then you may instruct SSL-Explorer to generate an untrusted certificate for use with the server. We will now walk through both options.

To generate an untrusted certificate:

Step 1 – Enter a new password for your certificate, enter the confirmation password and click update.

Step 2 – To generate your certificate, enter all of the following information making sure that you do not use punctuation characters such as commas anywhere in the values you enter.

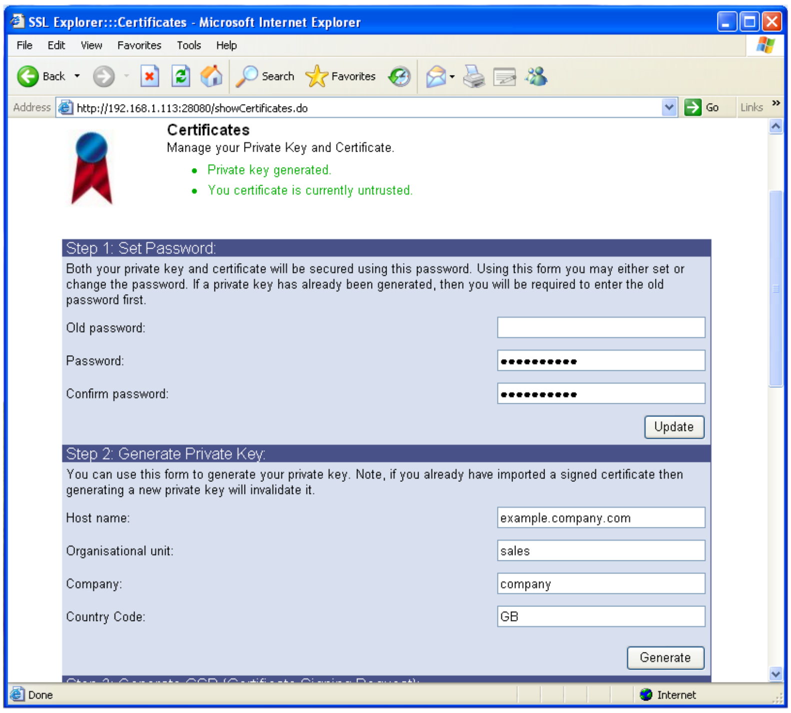
- **Hostname** – The software should have detected the server's IP address. If not, then enter the IP address or fully qualified domain name for the server here.

- **Organizational Unit** – This is a logical unit that specifies your hierarchy within your organization, for example "sales" or "accounts".

- **Company Name** – Enter the name of your company here.

- **Country Code** – This field contains a short code for the country in which you are currently located.

Next, click "generate". The SSL certificate will be generated and configured for use with the SSL-Explorer server and you can proceed to the next section.



http://192.168.1.113:28080/showCertificates.do

Certificates

Manage your Private Key and Certificate.

- Private key generated.
- You certificate is currently untrusted.

Step 1: Set Password:

Both your private key and certificate will be secured using this password. Using this form you may either set or change the password. If a private key has already been generated, then you will be required to enter the old password first.

Old password:

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

Update

Step 2: Generate Private Key:

You can use this form to generate your private key. Note, if you already have imported a signed certificate then generating a new private key will invalidate it.

Host name: example.company.com

Organisational unit: sales

Company: company

Country Code: GB

Generate

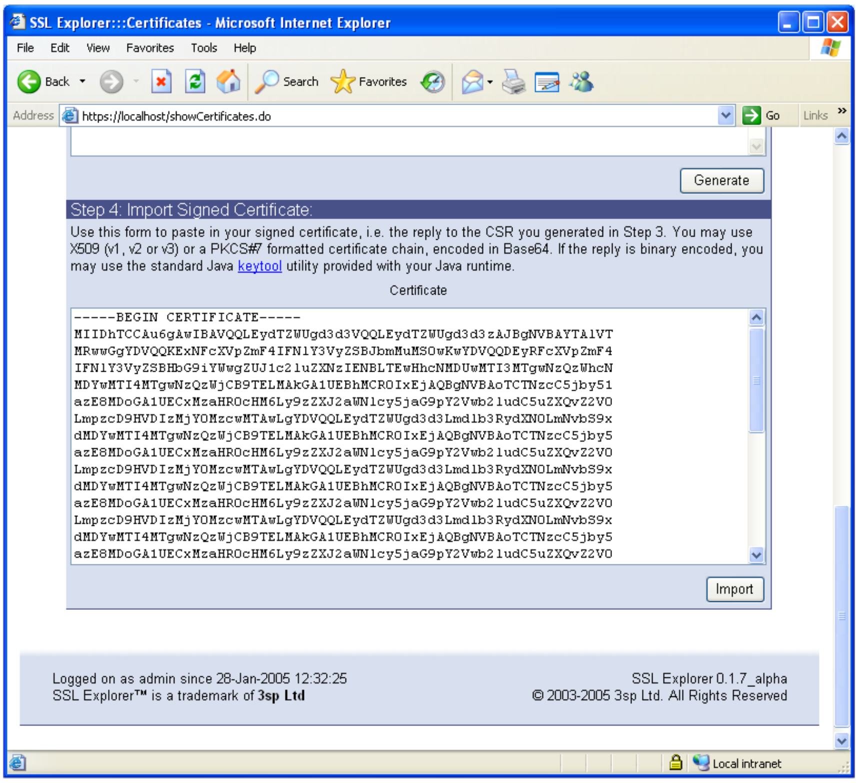
Security Advisory

It is important to remember that the SSL certificates generated by SSL-Explorer are untrusted. That is, they are not issued (and not signed) by a certificate authority (CA) such as Verisign or GeoTrust.

Step 3 (Optional) – You can use the private key you have just created to generate a certificate signing request which may be registered with a certification authority. The CA will use this data to generate you a trusted certificate which may be imported into SSL-Explorer.

To import a trusted certificate:

Step 1 – Once you have completed the certificate signing request detailed above, your CA will send you a signed certificate which you can paste into the textbox on step four of the certificate screen as follows:


SSL Explorer:::Certificates - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
https://localhost/showCertificates.do
Go
Links
Generate
Import
Local intranet

Step 4: Import Signed Certificate:

Use this form to paste in your signed certificate, i.e. the reply to the CSR you generated in Step 3. You may use X509 (v1, v2 or v3) or a PKCS#7 formatted certificate chain, encoded in Base64. If the reply is binary encoded, you may use the standard Java keytool utility provided with your Java runtime.

Certificate

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAu6gAwIBAVQQLEydTZWUgd3d3VQQLEydTZWUgd3d3zAJBgNVBAYTAlVT
MRwwGgYDVQQKExNFcXVpZmF4IFNlY3VyZSBJbmMuMSOwKwYDVQQDEyRFcXVpZmF4
IFNlY3VyZSBHbG9iYWwgZUJ1c2luZXNzIENBLTEwHhcNMDUwMTI3MTgwNzQzWhcN
MDYwMTI4MTgwNzQzWjCB9TELMAkGA1UEBhMCROIxEjAQBgNVBAoTCTNzcC5jby51
azE8MDoGA1UECxMzaHROcHM6Ly9zZXJ2aWNlcy5jaG9pY2Vwb2ludC5uZXQvZ2VO
LmpzcD9HVDIzMjYOMzcwMTAwLgYDVQQLEydTZWUgd3d3Lmdlb3RydXNOLmNvbS9x
dMDYwMTI4MTgwNzQzWjCB9TELMAkGA1UEBhMCROIxEjAQBgNVBAoTCTNzcC5jby5
azE8MDoGA1UECxMzaHROcHM6Ly9zZXJ2aWNlcy5jaG9pY2Vwb2ludC5uZXQvZ2VO
LmpzcD9HVDIzMjYOMzcwMTAwLgYDVQQLEydTZWUgd3d3Lmdlb3RydXNOLmNvbS9x
dMDYwMTI4MTgwNzQzWjCB9TELMAkGA1UEBhMCROIxEjAQBgNVBAoTCTNzcC5jby5
azE8MDoGA1UECxMzaHROcHM6Ly9zZXJ2aWNlcy5jaG9pY2Vwb2ludC5uZXQvZ2VO
LmpzcD9HVDIzMjYOMzcwMTAwLgYDVQQLEydTZWUgd3d3Lmdlb3RydXNOLmNvbS9x
dMDYwMTI4MTgwNzQzWjCB9TELMAkGA1UEBhMCROIxEjAQBgNVBAoTCTNzcC5jby5
azE8MDoGA1UECxMzaHROcHM6Ly9zZXJ2aWNlcy5jaG9pY2Vwb2ludC5uZXQvZ2VO
```

Logged on as admin since 28-Jan-2005 12:32:25
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2005 3sp Ltd. All Rights Reserved

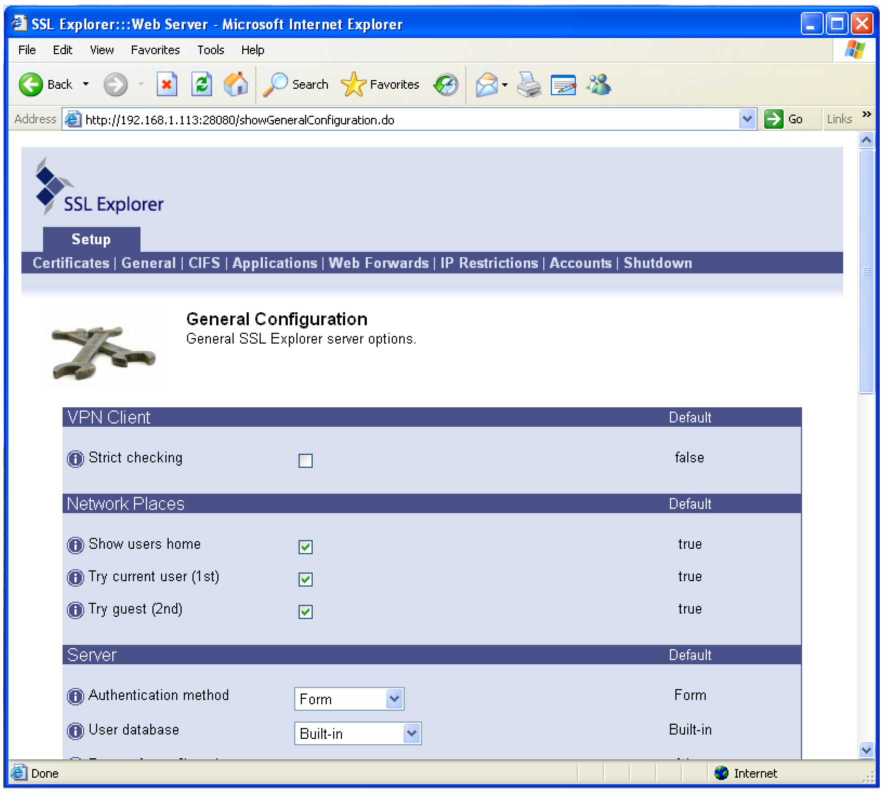
Your certificate has now been installed and is ready for use with SSL-Explorer! *Note that your users will now no longer be prompted by their browsers to accept an untrusted certificate. When using an untrusted certificate, your users will be prompted upon every connection to accept an untrusted certificate.*

2. Next, click the general tab at the top of the screen. Most values can be left to their defaults on this page. The most important things to remember are:

   - **Choose your user database** – Either Active Directory if you wish to use Windows accounts to log onto the system, or "built-in" to use SSL-Explorer's internal accounts database to store your user information.

   - **Configure your proxy settings** – HTTP or SOCKS proxy settings can be entered on this page. Leave blank if no proxy is used on your network.

If you chose to use the Built-In user database, please now skip to step 4.

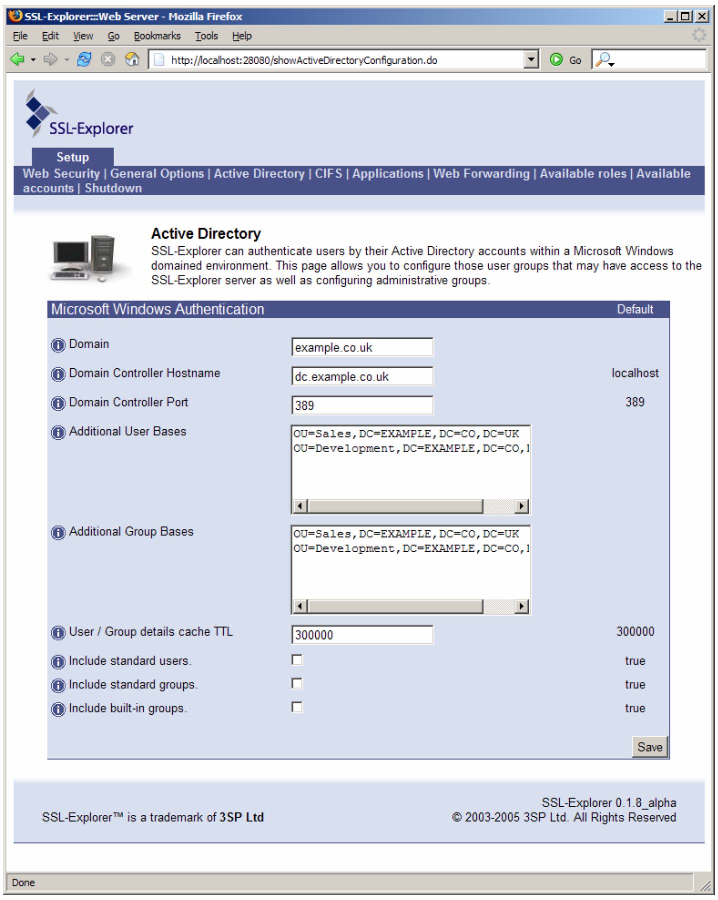

SSL Explorer:::Web Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.113:28080/showGeneralConfiguration.do
Go
Links
SSL Explorer
Setup
Certificates | General | CIFS | Applications | Web Forwards | IP Restrictions | Accounts | Shutdown
Done
Internet

General Configuration
General SSL Explorer server options.

VPN Client		Default
Strict checking	☐	false
Network Places		**Default**
Show users home	☑	true
Try current user (1st)	☑	true
Try guest (2nd)	☑	true
Server		**Default**
Authentication method	Form	Form
User database	Built-in	Built-in

Administrator Group(s) – Please enter here the Active Directory global group that will be designated as the administrator of the SSL-Explorer VPN server. Enter each group on a separate line, with no termination character. For example, *"Administrators"*. **If you forget this step, then you will not be able to access the administrative features when running SSL-Explorer in normal mode.**

3. Click the Active Directory tab. This screen contains configuration options that will allow your SSL-Explorer server to authenticate connecting users using their Microsoft Windows username/passwords.


SSL-Explorer::Web Server - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:28080/showActiveDirectoryConfiguration.do
Go
SSL-Explorer
Setup
Web Security | General Options | Active Directory | CIFS | Applications | Web Forwarding | Available roles | Available accounts | Shutdown
Save
Done

Active Directory

SSL-Explorer can authenticate users by their Active Directory accounts within a Microsoft Windows domained environment. This page allows you to configure those user groups that may have access to the SSL-Explorer server as well as configuring administrative groups.

Microsoft Windows Authentication		Default
Domain	example.co.uk	
Domain Controller Hostname	dc.example.co.uk	localhost
Domain Controller Port	389	389

Additional User Bases	OU=Sales,DC=EXAMPLE,DC=CO,DC=UK
	OU=Development,DC=EXAMPLE,DC=CO,I	

Additional Group Bases	OU=Sales,DC=EXAMPLE,DC=CO,DC=UK
	OU=Development,DC=EXAMPLE,DC=CO,I	

User / Group details cache TTL	300000	300000
Include standard users.	□	true
Include standard groups.	□	true
Include built-in groups.	□	true

SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Enter the following information here:

- **Domain** – This is the name assigned to your Microsoft Windows domain. E.g., "*example.co.uk*". The domain must be entered in lowercase.

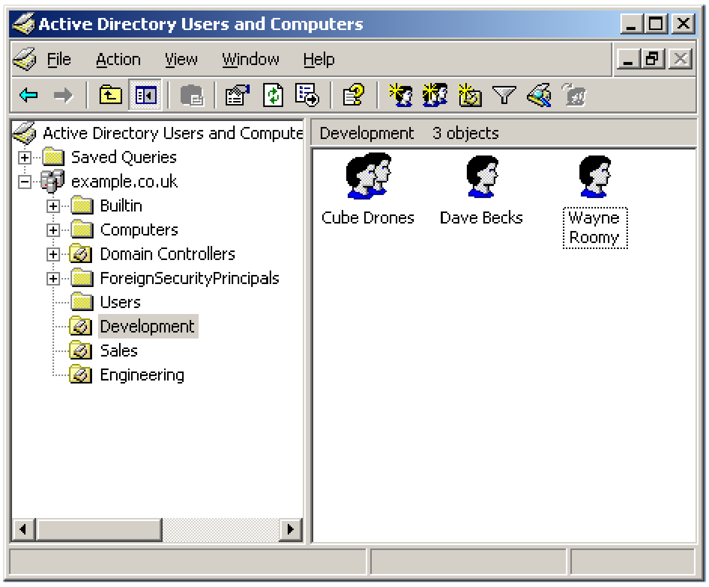
- **Domain Controller Hostname** – This is the fully qualified domain name for your Domain Controller (DC), e.g. "*dc.example.co.uk*".

Other Active Directory Options:

Domain Controller Port – This is the port number to use to communicate requests to and from the DC. Accept the default value.

Additional User Bases – If your users are located in multiple Active Directory Organizational Units (OUs) other than the default Users OU, then you must specify their location here. Otherwise they will not be able to log on to SSL-Explorer since SSL-Explorer will not query these non-standard OUs for accounts.

In our example domain pictured below, you can see that we have two users named Dave and Wayne in the Development OU.



In our example, our domain name is "example.co.uk" and our additional user bases are located in OUs named "Sales" and "Development". You will need to enter the constituent parts of the domain name in uppercase.

These user bases would be represented as follows:

```
OU=Sales,DC=EXAMPLE,DC=CO,DC=UK
OU=Development,DC=EXAMPLE,DC=CO,DC=UK
```

Separate each user base using the return key. There is no termination character used.

User and Group Base Syntax

Make sure that there is no white space between the elements of the user and group bases. There must be no spaces after the commas.

Additional Group Bases – In our example before, you'll notice an Active Directory group named "Cube Drones" in the Development OU. The two users present in that OU also happen to be group members.

In SSL-Explorer, if your users are members of custom groups that reside in non-standard OUs, then you must state these groups here – otherwise SSL-Explorer will not query these group bases for permissions. Again, you will need to enter the constituent parts of the domain name in uppercase.

For example:

```
CN=Cube Drones,OU=Development,DC=EXAMPLE,DC=CO,DC=UK
```

Separate each user base using the return key. There is no termination character used.

Include Standard Users – Include the standard user base 'CN=Users ....' built from the domain name. If you do not include these you will have to manually add your own user base string to the 'Additional user bases' list in order for SSL-Explorer to successfully locate your users.

Include Standard Groups – Include the standard group base 'CN=Users ....' built from the domain name. If you do not include these you will have to manually add your own group base string to the 'Additional group bases' list in order for SSL-Explorer to successfully locate group information to obtain user permissions.

Include Built-in Groups – Include the built-in group base 'CN=Builtin ....' built from the domain name. If you do not include these you will have to manually add your own group base string to the 'Additional group bases' list.

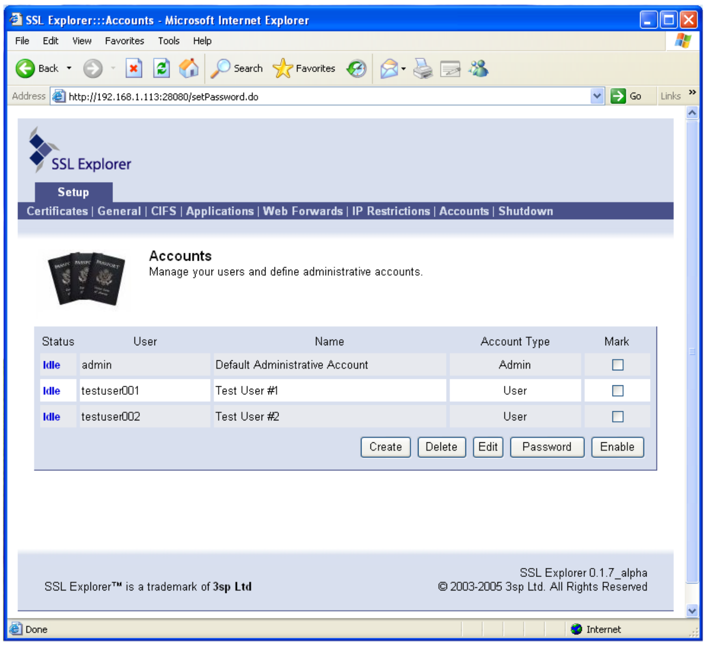
The Active Directory configuration process is now complete! Click shutdown and return to the appropriate installation section for your operating system.

🗁 Running the setup utility a second time

If you need to run SSL-Explorer in setup mode again, firstly make sure that you stop the SSL-Explorer service otherwise the setup utility will complain that the SSL port is in use and it will fail to start.

4. Click the accounts tab at the top of the screen. You will notice that a default administrative account has been created. **You should now change this password immediately – the default password is "admin".**

   Now you might want to create some accounts for your users. Account creation is dealt with in the next section.


SSL Explorer:::Accounts - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
SSL Explorer
Setup
Certificates | General | CIFS | Applications | Web Forwards | IP Restrictions | Accounts | Shutdown
Done
Internet

http://192.168.1.113:28080/setPassword.do

Accounts

Manage your users and define administrative accounts.

Status	User	Name	Account Type	Mark
Idle	admin	Default Administrative Account	Admin	□
Idle	testuser001	Test User #1	User	□
Idle	testuser002	Test User #2	User	□

Create Delete Edit Password Enable

SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2005 3sp Ltd. All Rights Reserved

The Built-In user database configuration process is complete! Click shutdown and return to the appropriate installation section for your operating system.

Running the setup utility a second time

If you need to run SSL-Explorer in setup mode again, firstly make sure that you stop the SSL-Explorer service otherwise the setup utility will complain that the SSL port is in use and it will fail to start.

SSL-Explorer on Other Linux Distributions

At this moment in time, the use of SSL-Explorer is only officially supported on the Red Hat Linux 8.0 or later platform. Due to the number of available distributions and time constraints we cannot claim to support all, but we are aiming to make full documentation available in time for more popular distributions.

The following table describes the steps needed to install SSL-Explorer on the Linux distributions that we have tested.

Platform	Installer	Post Install	Start Service	Stop Service	Un-install	SSL-Explorer Setup mode	SSL-Explorer Console mode
RedHat	GUI (preferred when a GUI is available)	Installer does everything	Either RH service GUI tool or "service sslexplorer start"	Either RH service GUI tool or "service sslexplorer stop"	Run uninstall	Run setup-sslexplorer.	Run sslexplorer-console
RedHat	RPM (for command line installs)	Run [install-location]/platforms/linux/install-service, then setup-sslexplorer	Either RH service GUI tool or "service sslexplorer start"	Either RH service GUI tool or "service sslexplorer stop"	Run [install-location]/platforms/linux/install-service -u then run rpm --erase sslexplorer	Run setup-sslexplorer.	Run sslexplorer-console
Generic Unix Linux	Generic Unix / Linux	Run ./platforms/[platform]/install-service if available, then run ./setup-sslexplorer	If install-service available, start service in way appropriate for platform	If install-service available, start service in way appropriate for platform	Run ./platforms/[platform]/install-service -u if available, then remove installation directory	Run ./setup-sslexplorer	Run ./sslexplorer-console
Slackware	Slackware Package	Run setup-sslexplorer	/etc/rc.d/rc.sslexplorer start	/etc/rc.d/rc.sslexplorer start	removepkg sslexplorer-0.1.5-i386-1bps	Run setup-sslexplorer.	Run sslexplorer-console
Slackware	GUI	Installer does everything	/etc/rc.d/rc.sslexplorer start	/etc/rc.d/rc.sslexplorer start	Run uninstall	Run setup-sslexplorer	Run sslexplorer-console

Chapter

4

Security using Role Based Access Control

Configuring permissions using the concept of RBAC.

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Keyboard exercise
- 📖 Workbook review

Granular Permissions

With release 0.1.8 of SSL-Explorer, enhanced user permissions were introduced to allow more effective user rights management. User's may be granted or denied access to certain features, and greater control over your user's protocol tunnelling rights has been implemented.

RBAC uses the concept of user roles and groups to allow for a more intuitive and efficient administrative experience

The concept of Role Based Access Control is used to mirror your own organizations hierarchical divisions more accurately. Instead of maintaining individual permission lists for each of your users; role-based permissions allow you to assign your entire sales department an alternative set of SSL-Explorer permissions to your development team.

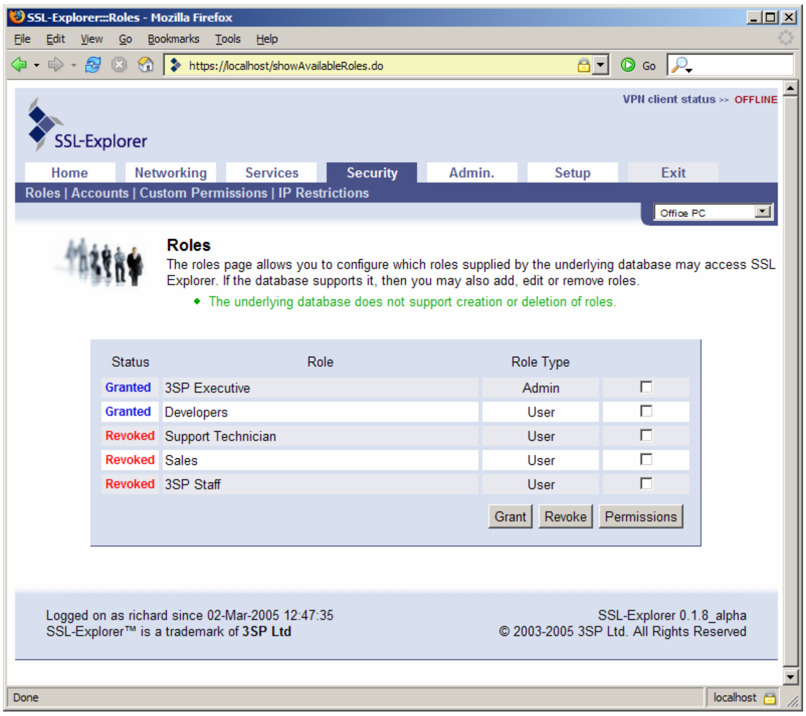
When Active Directory user authentication is configured, your Active Directory user groups are defined in SSL-Explorer as roles and permissions for each of these roles may be assigned. All users within these roles will inherit the permissions you define, and individual accounts within these roles may be granted/denied access to the SSL-Explorer server.

When using the built-in accounts database, you must create your user roles and assign users to these groups manually. In this section, we'll walk through the permissions and rights enforcement using both user databases.

Configuring Active Directory Roles

In the web-based setup procedure, you entered information necessary for SSL-Explorer to communicate with your Microsoft Windows domain controller. In order to query Active Directory and assign permissions to roles, you will first need to log into SSL-Explorer using your domain credentials.

Once logged in, click the security tab at the top of the screen.


SSL-Explorer::Roles - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showAvailableRoles.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Office PC
Done
localhost

Roles

The roles page allows you to configure which roles supplied by the underlying database may access SSL Explorer. If the database supports it, then you may also add, edit or remove roles.

- The underlying database does not support creation or deletion of roles.

Status	Role	Role Type	
Granted	3SP Executive	Admin	□
Granted	Developers	User	□
Revoked	Support Technician	User	□
Revoked	Sales	User	□
Revoked	3SP Staff	User	□

Logged on as richard since 02-Mar-2005 12:47:35
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

You will notice that the role that you defined as an administrative role in setup has the role type of 'admin'. From here you can choose other roles that may be granted access to the SSL-Explorer server and assign permissions to these roles.

Let's assign another role with access to the system. Select one of the 'revoked' roles in the list and click 'grant'. SSL-Explorer has now granted logon access to this role, although since no permissions have yet been defined for the role, users connecting to the system will have no effective rights to do anything!

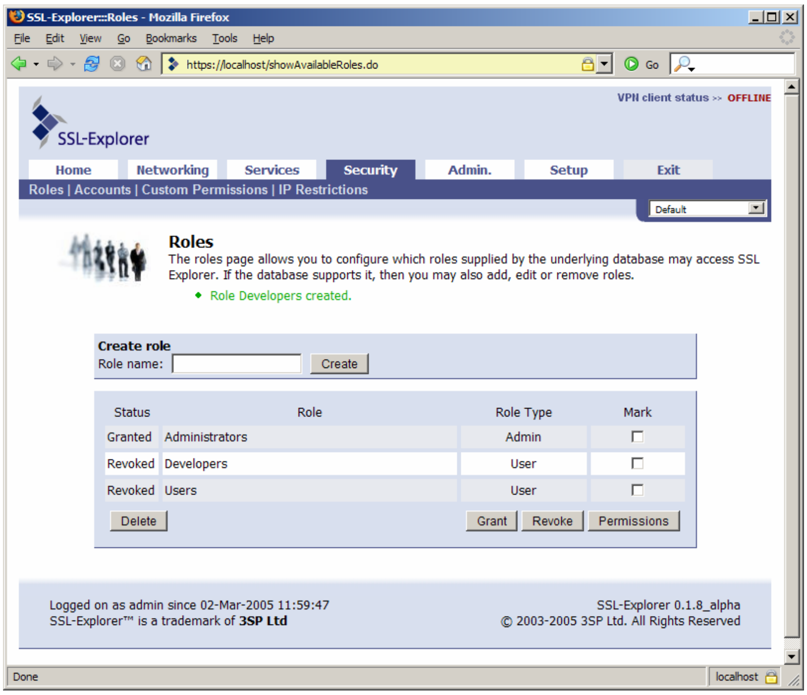
Select the role you have just granted and click 'permissions' to enter the role permissions screen and skip to page 29.

Configuring Roles with the Built-in Database

When using the built-in SSL-Explorer database, you will need to create your roles manually. This may be done as part of setup mode or whilst already logged into the system under an administrative account.

Click the 'available roles' tab at the top of the screen to enter the role creation screen. Create a number of roles here to reflect your organisations hierarchical boundaries. Here we have created a 'Developers' role, and this has been set up with a status of 'revoked', meaning that this role does not have any access by default to the SSL-Explorer VPN server.

Select the new role and click 'grant' to allow logon access for the 'Developers' role.


SSL-Explorer:::Roles - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showAvailableRoles.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Default
Done
localhost

Roles

The roles page allows you to configure which roles supplied by the underlying database may access SSL Explorer. If the database supports it, then you may also add, edit or remove roles.

- Role Developers created.

Create role

Role name: [ ] Create

Status	Role	Role Type	Mark
Granted	Administrators	Admin	□
Revoked	Developers	User	□
Revoked	Users	User	□

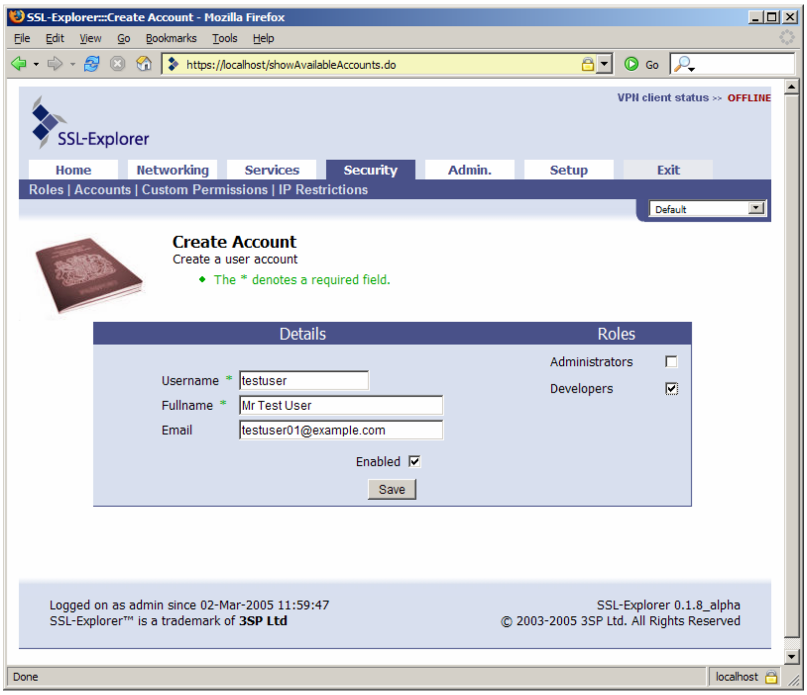
Delete Grant Revoke Permissions

Logged on as admin since 02-Mar-2005 11:59:47
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Now we need to assign some users to this role, so click the 'available accounts' tab at the top of the screen.

Here you need to create a few users and assign them to your new role by selecting the appropriate role(s) on the right hand side of the screen.


SSL-Explorer::Create Account - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showAvailableAccounts.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Default
Done
localhost

Create Account
Create a user account
- The * denotes a required field.

Details		Roles	
Username *	testuser	Administrators	□
Fullname *	Mr Test User	Developers	☑
Email	testuser01@example.com		

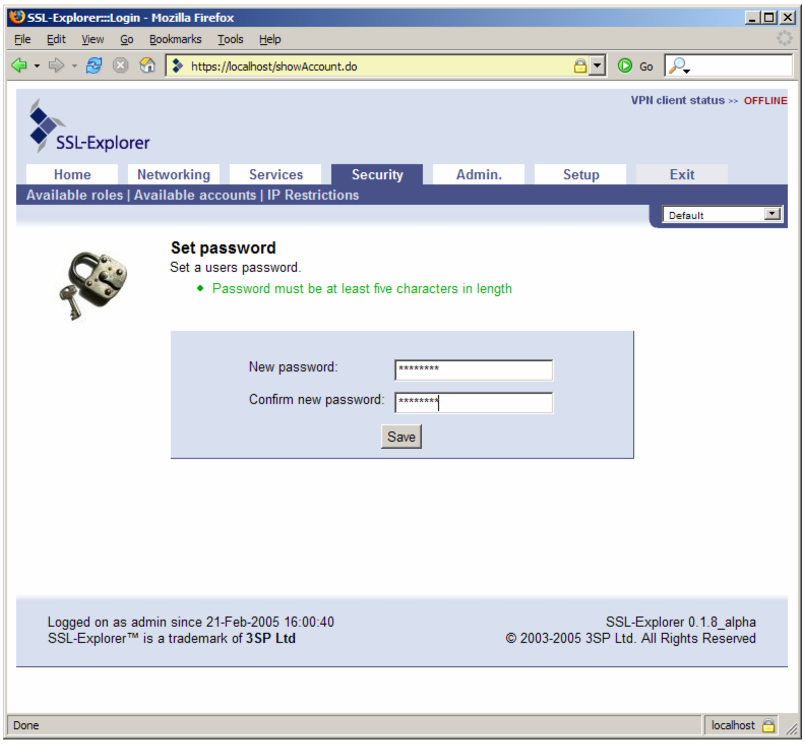
Enabled ☑

Save

Logged on as admin since 02-Mar-2005 11:59:47
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Click save, and then assign the user a password.


SSL-Explorer::Login - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showAccount.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Available roles | Available accounts | IP Restrictions
Default
Done
localhost

Set password
Set a users password.
- Password must be at least five characters in length

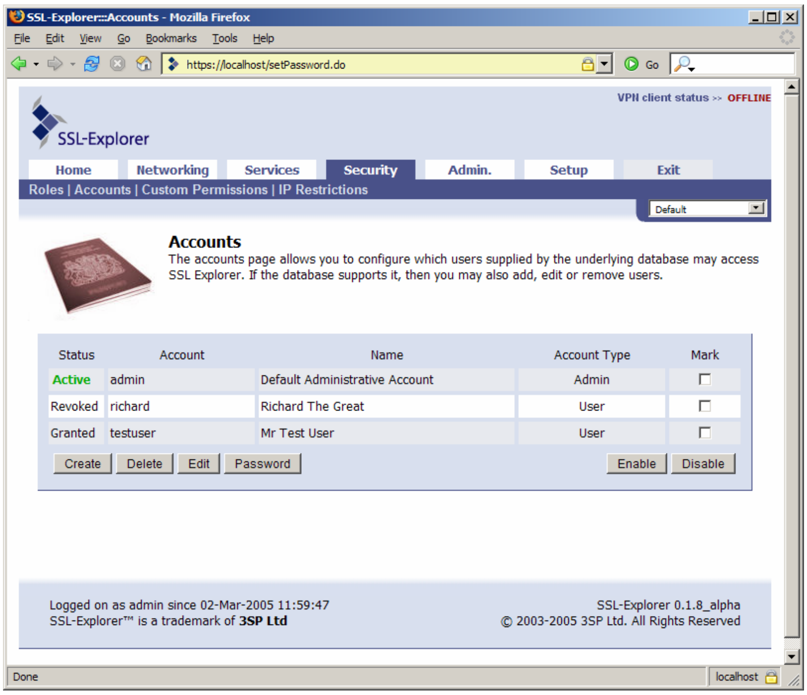
New password: ********
Confirm new password: ********

Save

Logged on as admin since 21-Feb-2005 16:00:40
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Your new user has now been created and assigned our example 'Developers' role.



SSL-Explorer::Accounts - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/setPassword.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Default

Accounts

The accounts page allows you to configure which users supplied by the underlying database may access SSL Explorer. If the database supports it, then you may also add, edit or remove users.

Status	Account	Name	Account Type	Mark
Active	admin	Default Administrative Account	Admin	□
Revoked	richard	Richard The Great	User	□
Granted	testuser	Mr Test User	User	□

Create
Delete
Edit
Password
Enable
Disable

Logged on as admin since 02-Mar-2005 11:59:47
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

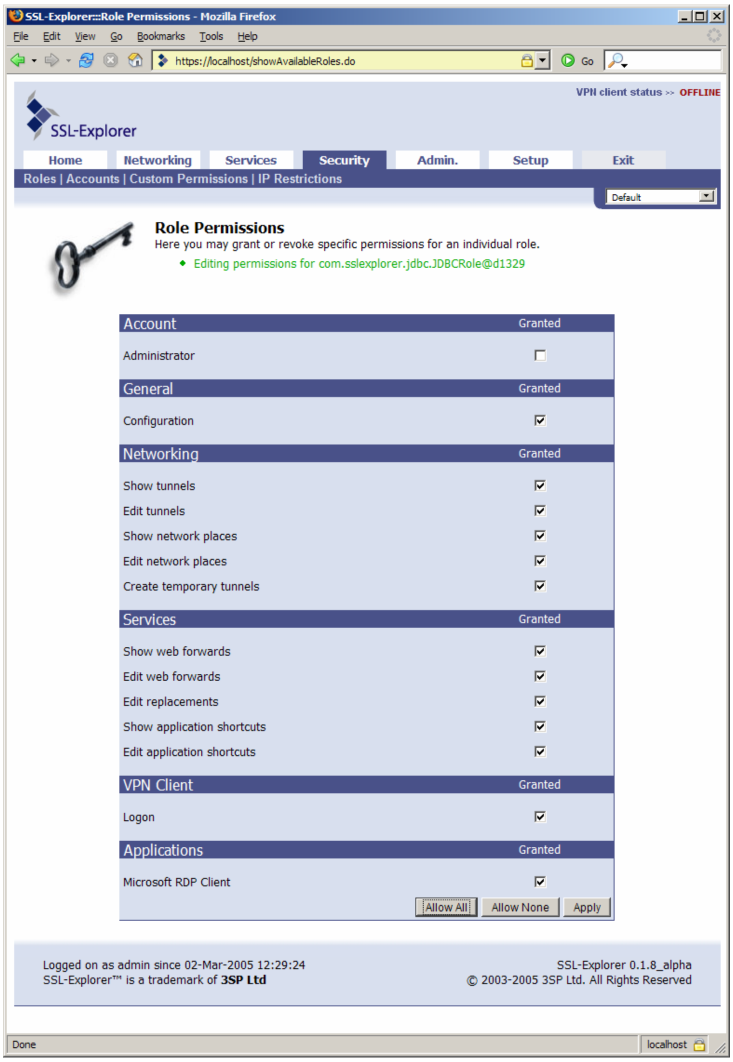
Although SSL-Explorer has granted logon access to this role, since no permissions have yet been defined for the role, users connecting to the system will have no effective rights to do anything! Go back to the available roles screen, select your new role and click 'permissions' to enter the role permissions screen.

Assigning Role Permissions

In the role permissions screen, you can define the networking, services and applications that your role may have access to, along with further options to allow/disallow the starting of the VPN client. These permissions will apply to every user that is a member of the role.

For users that are members of more than one role, the cumulative permissions that were assigned to each role are used as the effective permissions. This means that say you created two roles where the first allowed only the 'edit tunnels' permission and the second the 'create tunnels' permission – users that belong to both roles will have effective permissions to create and edit tunnels.

Select 'allow all' to grant full non-administrative permissions, or choose your own set of permissions applicable to that role.


SSL-Explorer::Role Permissions - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showAvailableRoles.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Default
Allow All
Allow None
Apply
Done
localhost

Role Permissions
Here you may grant or revoke specific permissions for an individual role.
- Editing permissions for com.sslexplorer.jdbc.JDBCRole@d1329

Account	Granted
Administrator	□
General	**Granted**
Configuration	☑
Networking	**Granted**
Show tunnels	☑
Edit tunnels	☑
Show network places	☑
Edit network places	☑
Create temporary tunnels	☑
Services	**Granted**
Show web forwards	☑
Edit web forwards	☑
Edit replacements	☑
Show application shortcuts	☑
Edit application shortcuts	☑
VPN Client	**Granted**
Logon	☑
Applications	**Granted**
Microsoft RDP Client	☑

Logged on as admin since 02-Mar-2005 12:29:24
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

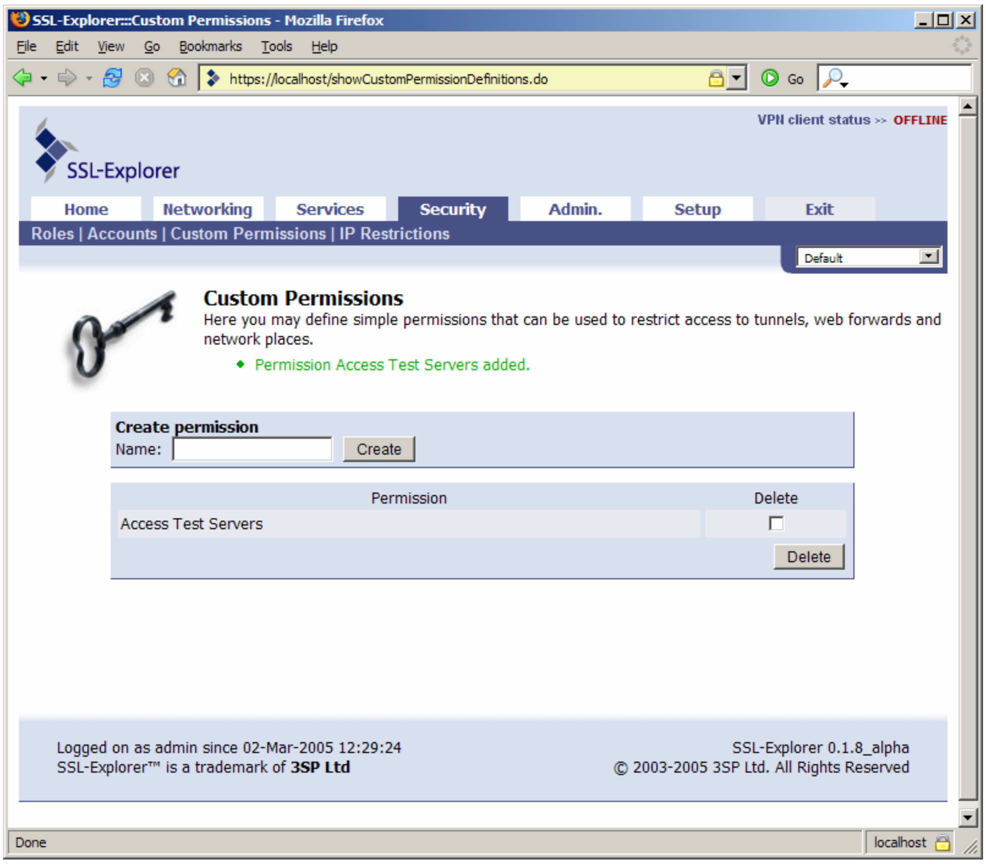
Click apply to save the role permissions settings and try logging into your new users account to see the role based permissions in action.

Custom Permissions

You can create custom permissions that can be associated with applications and tunnels that you set up on SSL-Explorer. These custom permissions may then be granted at the role level to allow certain roles to have access to certain services whilst denying access to others.

1. Create Custom Permission

We are going to create a custom permission to allow our development team access to a number of test servers using Terminal Services. In our example below, we have created a permission of "Access Test Servers".



SSL-Explorer:::Custom Permissions - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showCustomPermissionDefinitions.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Default
Create
Delete
Done
localhost

Custom Permissions

Here you may define simple permissions that can be used to restrict access to tunnels, web forwards and network places.

- Permission Access Test Servers added.

Create permission

Name:

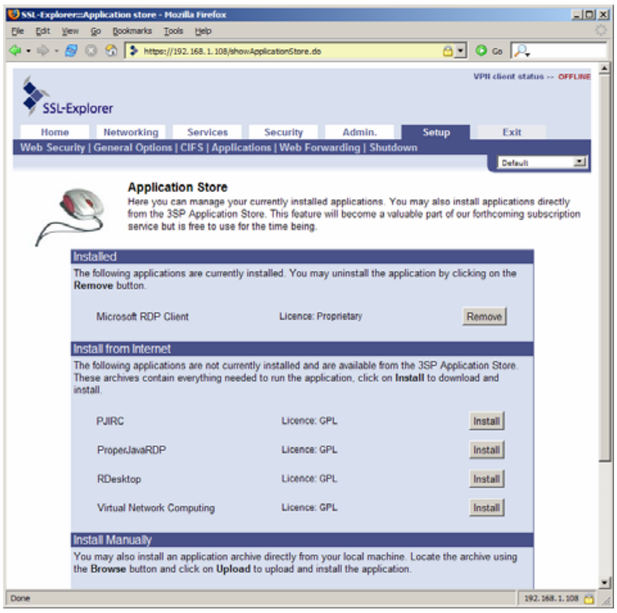
Permission	Delete
Access Test Servers	□

Logged on as admin since 02-Mar-2005 12:29:24
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

2. Install Application

Since we're using Terminal Services, we next need to set up the Microsoft RDP Client for use on the SSL-Explorer VPN. Click the Setup tab at the top of the screen and then choose the submenu named 'Applications'. Click the install button for the 'Microsoft RDP Client'.


SSL-Explorer::Application store - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.108/showApplicationStore.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Web Security | General Options | CIFS | Applications | Web Forwarding | Shutdown
Default
Done
192.168.1.108

Application Store

Here you can manage your currently installed applications. You may also install applications directly from the 3SP Application Store. This feature will become a valuable part of our forthcoming subscription service but is free to use for the time being.

Installed

The following applications are currently installed. You may uninstall the application by clicking on the **Remove** button.

Microsoft RDP Client	Licence: Proprietary	Remove

Install from Internet

The following applications are not currently installed and are available from the 3SP Application Store. These archives contain everything needed to run the application, click on **Install** to download and install.

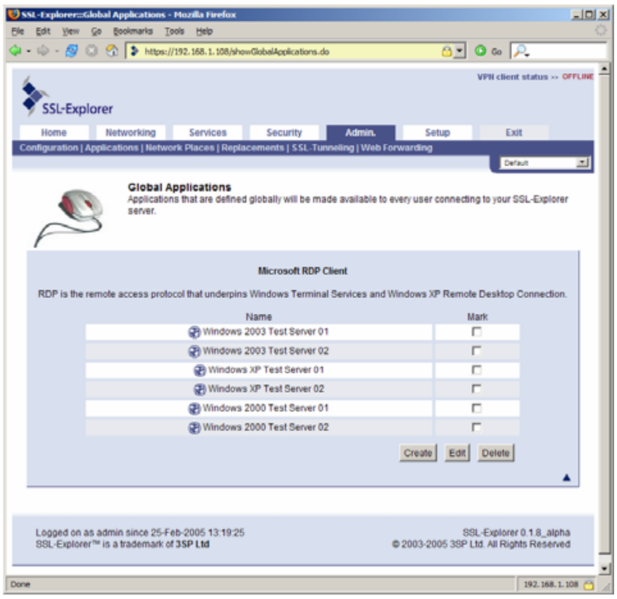
PJIRC	Licence: GPL	Install
ProperJavaRDP	Licence: GPL	Install
RDesktop	Licence: GPL	Install
Virtual Network Computing	Licence: GPL	Install

Install Manually

You may also install an application archive directly from your local machine. Locate the archive using the **Browse** button and click on **Upload** to upload and install the application.

3. Create Application Shortcuts and Associate with permission

Click the Admin tab and then choose 'Applications'. In this screen you will notice a section for the Microsoft RDP client that you have just installed. Here we have created several 'Global Application Shortcuts' to our test server environment.


SSL-Explorer::Global Applications - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.108/showGlobalApplications.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Configuration | Applications | Network Places | Replacements | SSL-Tunneling | Web Forwarding
Default
Create Edit Delete
Done
192.168.1.108

Global Applications

Applications that are defined globally will be made available to every user connecting to your SSL-Explorer server.

Microsoft RDP Client

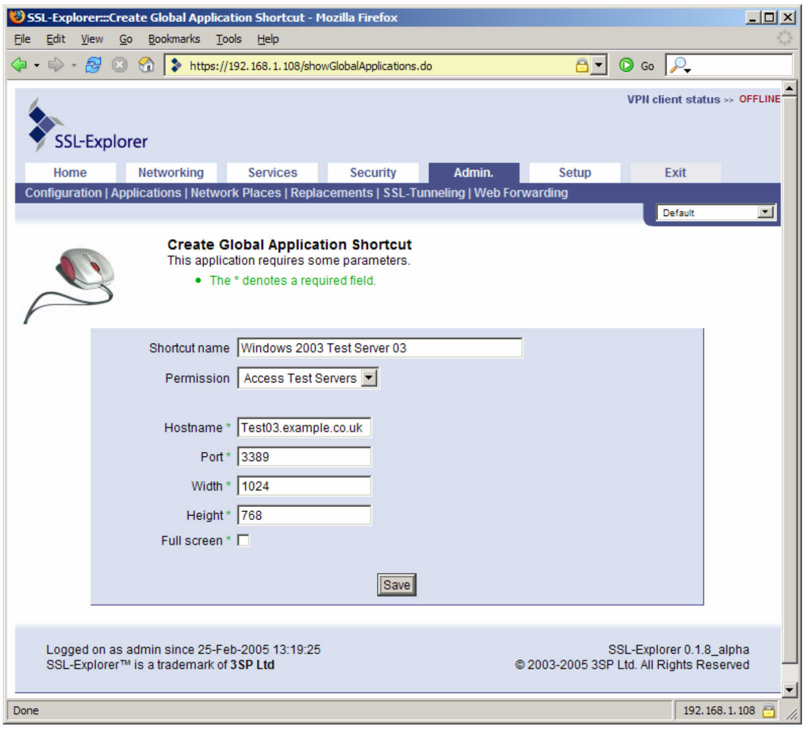
RDP is the remote access protocol that underpins Windows Terminal Services and Windows XP Remote Desktop Connection.

Name	Mark
Windows 2003 Test Server 01	□
Windows 2003 Test Server 02	□
Windows XP Test Server 01	□
Windows XP Test Server 02	□
Windows 2000 Test Server 01	□
Windows 2000 Test Server 02	□

Logged on as admin since 25-Feb-2005 13:19:25
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

When you create your application shortcut, you will notice a drop down listbox named permission appears. Selecting a custom permission in here will associate this application shortcut with only those roles that have been granted the custom permission.


SSL-Explorer::Create Global Application Shortcut - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.108/showGlobalApplications.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Configuration | Applications | Network Places | Replacements | SSL-Tunneling | Web Forwarding
Default
Save
Done
192.168.1.108

Create Global Application Shortcut

This application requires some parameters.

- The * denotes a required field.

Shortcut name: Windows 2003 Test Server 03

Permission: Access Test Servers

Hostname *: Test03.example.co.uk

Port *: 3389

Width *: 1024

Height *: 768

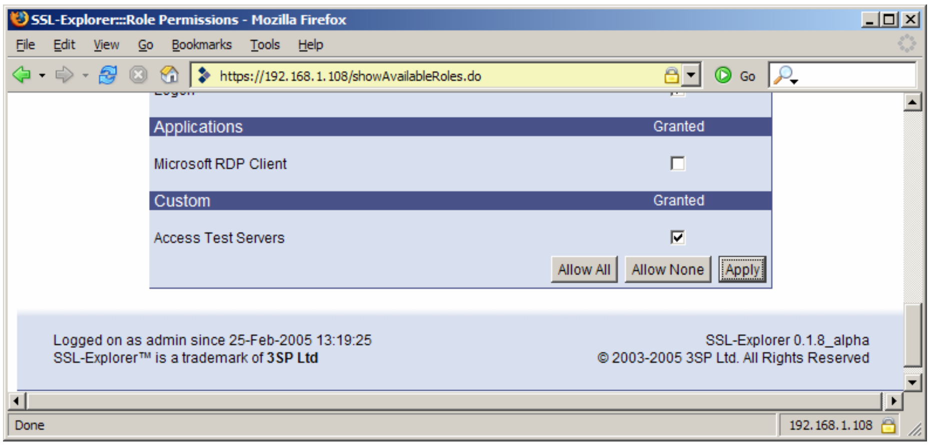
Full screen *: □

Logged on as admin since 25-Feb-2005 13:19:25
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

4. Associate Role with Custom Permission

Next, you need to update your Developers role to grant them access to the new custom permission. Choose the security tab, click available roles and edit the permissions on your Developers role. At the bottom of the list, you'll notice your new custom permission has appeared. Check the box for the new 'Access Test Servers' custom permission and also check the box by 'Microsoft RDP Client' to allow the role RDP access then click apply.


SSL-Explorer::Role Permissions - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.1.108/showAvailableRoles.do
Go
Allow All
Allow None
Apply
Done
192.168.1.108

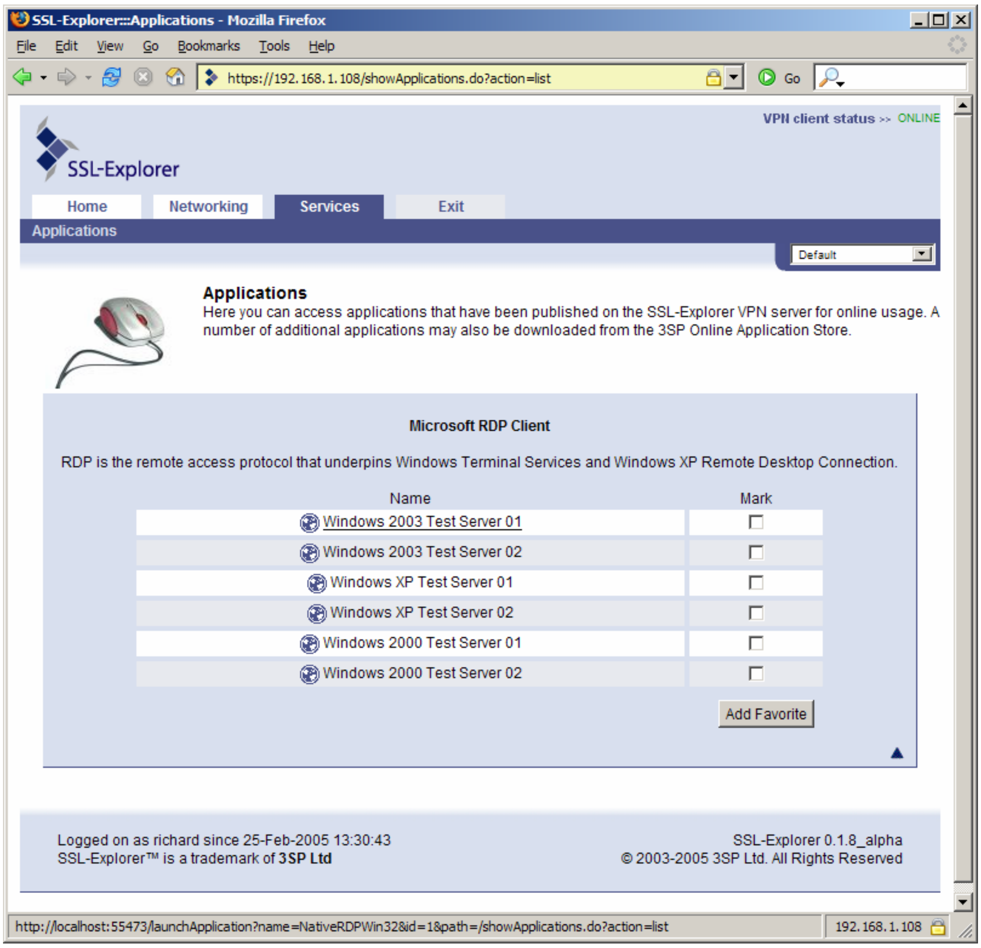
Applications	Granted
Microsoft RDP Client	□
Custom	**Granted**
Access Test Servers	☑

Logged on as admin since 25-Feb-2005 13:19:25
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

5. Test the Custom Role

Try logging in as your new user to see the custom permission settings in action. Select the applications menu under services and expand the Microsoft RDP Client area and you will see all of the test server links that you created earlier. These links are only visible to members of the Developers role.


SSL-Explorer:::Applications - Mozilla Firefox
File
Edit
View
Go
Bookmarks
Tools
Help
https://192.168.1.108/showApplications.do?action=list
Go
VPN client status >> ONLINE
SSL-Explorer
Home
Networking
Services
Exit
Applications
Default
Add Favorite

Applications
Here you can access applications that have been published on the SSL-Explorer VPN server for online usage. A number of additional applications may also be downloaded from the 3SP Online Application Store.

Microsoft RDP Client

RDP is the remote access protocol that underpins Windows Terminal Services and Windows XP Remote Desktop Connection.

Name	Mark
Windows 2003 Test Server 01	□
Windows 2003 Test Server 02	□
Windows XP Test Server 01	□
Windows XP Test Server 02	□
Windows 2000 Test Server 01	□
Windows 2000 Test Server 02	□

Logged on as richard since 25-Feb-2005 13:30:43
SSL-Explorer™ is a trademark of **3SP Ltd**

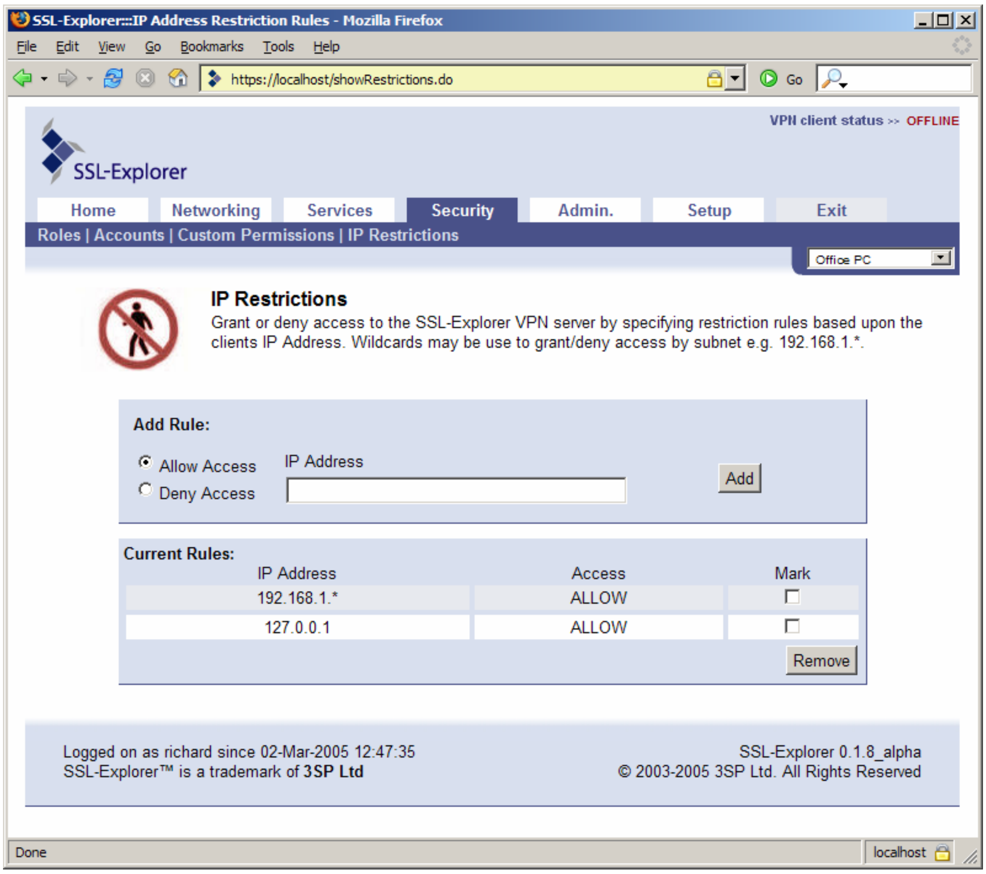
SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

http://localhost:55473/launchApplication?name=NativeRDPWin32&id=1&path=/showApplications.do?action=list
192.168.1.108

IP Restrictions

SSL-Explorer may be configured to grant or deny access to users based upon their IP address. This is useful in situations where you know the IP addresses of all clients that require the use of the VPN server. IP addresses may be specified for restriction by using wildcards if necessary.

The example below shows SSL-Explorer set up for internal company usage and will only accept connections from the local subnet 192.168.1.* and the local PC, 127.0.0.1.



SSL-Explorer::IP Address Restriction Rules - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showRestrictions.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Roles | Accounts | Custom Permissions | IP Restrictions
Office PC

IP Restrictions

Grant or deny access to the SSL-Explorer VPN server by specifying restriction rules based upon the clients IP Address. Wildcards may be use to grant/deny access by subnet e.g. 192.168.1.*.

Add Rule:

● Allow Access
○ Deny Access

IP Address

[Add]

Current Rules:

IP Address	Access	Mark
192.168.1.*	ALLOW	□
127.0.0.1	ALLOW	□

[Remove]

Logged on as richard since 02-Mar-2005 12:47:35
SSL-Explorer™ is a trademark of **3SP Ltd**

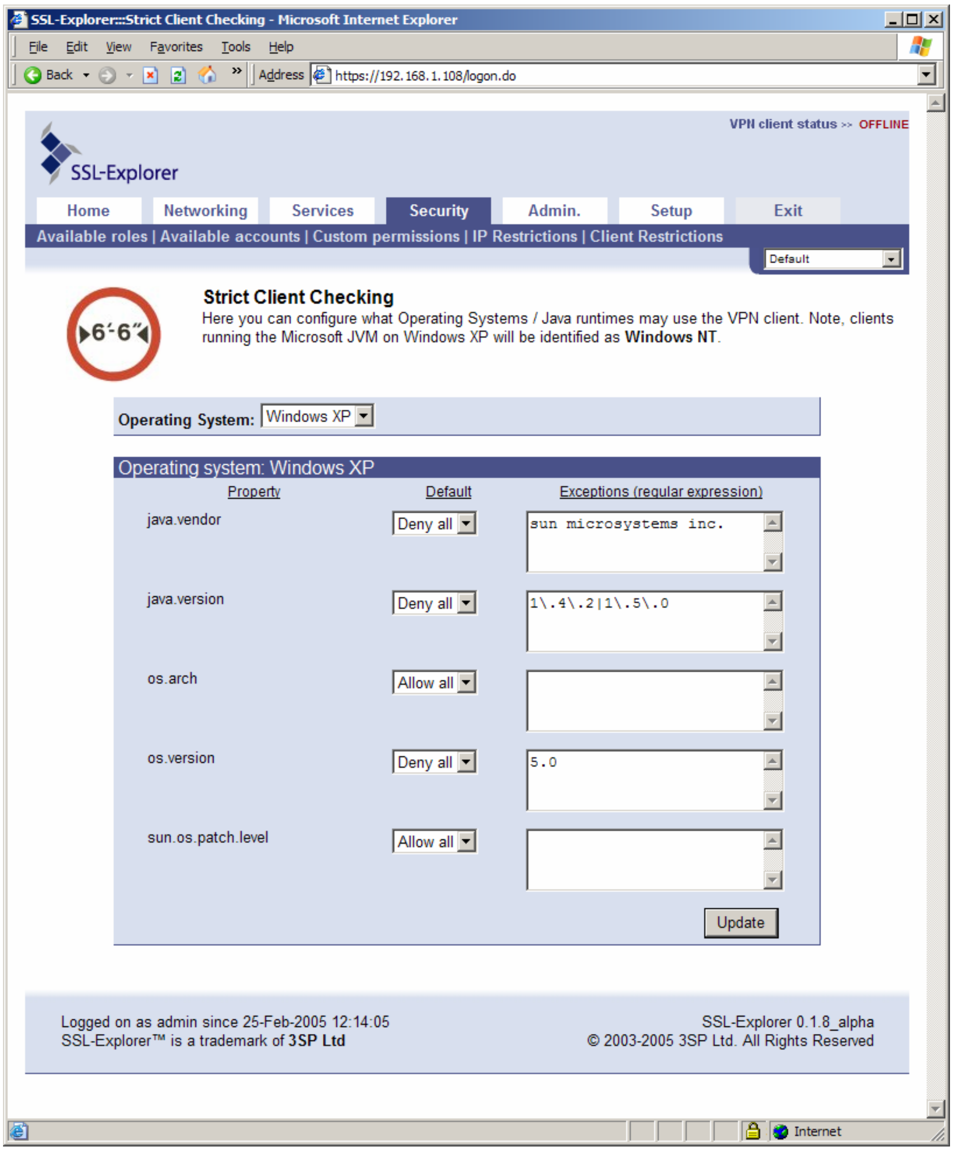
SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Strict Client Checking

You can configure SSL-Explorer to grant or deny access to connecting VPN clients based upon the values of system properties[4] returned by their Java Virtual Machine. This feature is enabled in the global configuration page, and once enabled a new submenu named 'Client Restrictions' appears in the security tab.

This can be used to restrict access to your VPN server to unsupported operating systems, clients with outdated operating systems or older versions of the JVM.

Five properties are available that may be queried using regular expressions (see page 60). In the example below, we are granting access to Windows XP machines running the Sun Microsystems JVM versions 1.4.2 or 1.5.0 only.


SSL-Explorer::Strict Client Checking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://192.168.1.108/logon.do
VPN client status >> OFFLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
Available roles | Available accounts | Custom permissions | IP Restrictions | Client Restrictions
Default
Internet

Strict Client Checking

Here you can configure what Operating Systems / Java runtimes may use the VPN client. Note, clients running the Microsoft JVM on Windows XP will be identified as **Windows NT**.

Operating System: Windows XP

Operating system: Windows XP

Property	Default	Exceptions (regular expression)
java.vendor	Deny all	sun microsystems inc.
java.version	Deny all	1\.4\.2|1\.5\.0
os.arch	Allow all	
os.version	Deny all	5.0
sun.os.patch.level	Allow all	

Update

Logged on as admin since 25-Feb-2005 12:14:05
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

[4] For a full list of query-able Java system properties see http://www.tolstoy.com/samizdat/sysprops.html

Chapter 5

Starting the Server for the First Time

Get familiarised with the SSL-Explorer interface.

ICON KEY

🗀 Valuable information

✎ Test your knowledge

💻 Keyboard exercise

🕮 Workbook review

Let's take a look around…

We'll begin by introducing you to the SSL-Explorer interface.

The SSL-Explorer interface is divided into three logical user components and three additional tabs for administrative users.

It is not prudent to consider installing a security solution onto a Windows system without first ensuring that the system is firstly up-to-date with all published service packs and hot-fixes.

- **Home Page** – This page contains information on getting started with SSL-Explorer. A facility to launch the VPN client, and access to services that are set as your 'favourites'.

- **Networking** – Access to network resources such as the Microsoft Windows filesystem browser and the port forwarding configuration screen.

- **Services** – Access to published intranet resources using the secure proxy feature of SSL-Explorer. Both Java-based and native applications may also be published by the SSL-Explorer administrator for remote deployment to clients.

- **Security (Admin only)** – Configure which accounts may have access to the system and what they may do whilst logged on. IP restrictions are also configurable here.

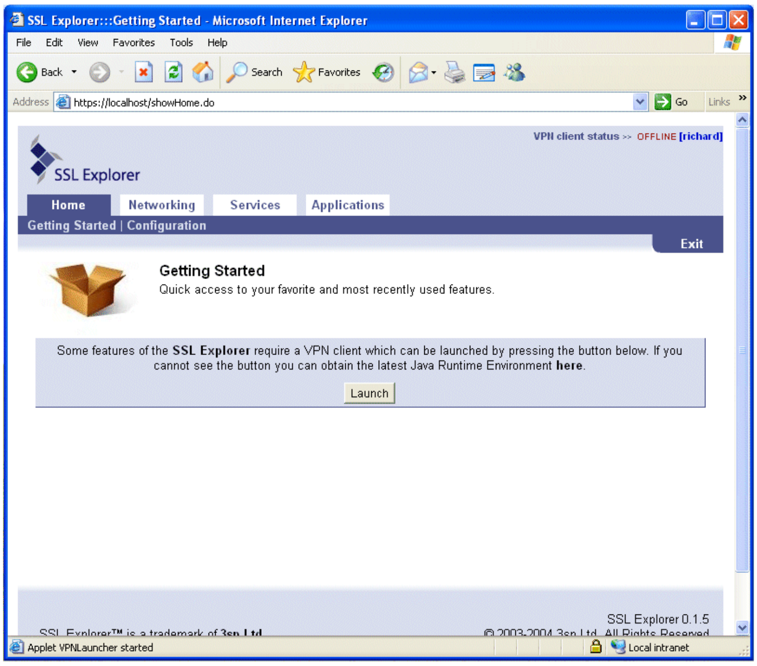
- **Admin (Admin only)** – Define global configuration settings that are available to all users such as port forwarding and web forwards.

- **Setup (Admin only)** – Setup applications, networking properties, Active Directory and web security settings.

Home Page

The first screen you will see upon successfully logging into SSL-Explorer is the Getting Started page. This page is intended to provide quick access to pre-configured ‘favourite’ connections. A later tutorial will introduce you to the concept of creating ‘favourite connections’.

Some features of the SSL-Explorer – namely port forwarding, single-site web forwarding and application deployment – will require the VPN applet to be launched. An option is provided here to start the VPN client.



https://localhost/showHome.do

Getting Started

Quick access to your favorite and most recently used features.

Some features of the **SSL Explorer** require a VPN client which can be launched by pressing the button below. If you cannot see the button you can obtain the latest Java Runtime Environment **here**.

SSL Explorer™ is a trademark of 3sp Ltd.

SSL Explorer 0.1.5

© 2003-2004 3sp Ltd. All Rights Reserved

Applet VPNLauncher started

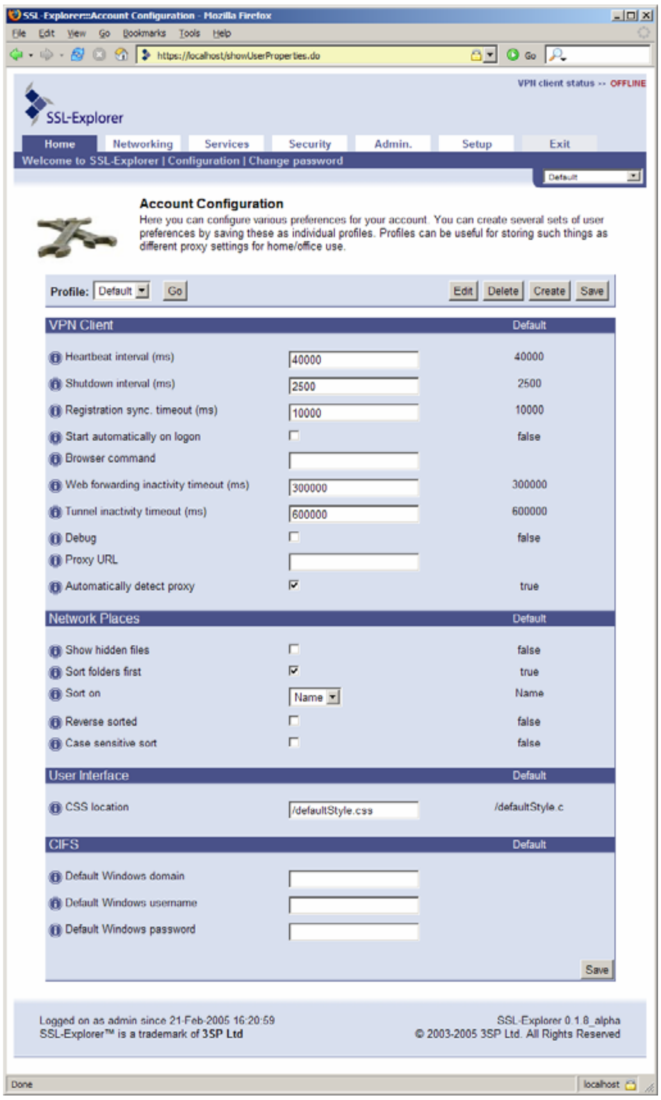
🗁 The SSL-Explorer VPN Client

The VPN client is a small Java applet that provides access to advanced SSL tunnelling features required by certain features of the SSL-Explorer server. More information on the VPN client and how it interacts with the SSL-Explorer server and your web browser can be found in Chapter 7.

Click on the configuration sub-menu item to enter the main SSL-Explorer configuration screen

Home Page – Configuration Screen

Clicking on the configuration menu item brings you to the main SSL-Explorer configuration screen where you can set options relating to the VPN client, the Microsoft Windows filesystem browser and the user interface. The configuration options here are specific for the currently logged-on user only.


SSL-Explorer:::Account Configuration - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showUserProperties.do
Go
VPN client status ›› OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Welcome to SSL-Explorer | Configuration | Change password
Default

Account Configuration

Here you can configure various preferences for your account. You can create several sets of user preferences by saving these as individual profiles. Profiles can be useful for storing such things as different proxy settings for home/office use.

Profile: Default ▾ Go   Edit Delete Create Save

VPN Client		Default
Heartbeat interval (ms)	40000	40000
Shutdown interval (ms)	2500	2500
Registration sync. timeout (ms)	10000	10000
Start automatically on logon	□	false
Browser command		
Web forwarding inactivity timeout (ms)	300000	300000
Tunnel inactivity timeout (ms)	600000	600000
Debug	□	false
Proxy URL		
Automatically detect proxy	☑	true

Network Places		Default
Show hidden files	□	false
Sort folders first	☑	true
Sort on	Name ▾	Name
Reverse sorted	□	false
Case sensitive sort	□	false

User Interface		Default
CSS location	/defaultStyle.css	/defaultStyle.c

CIFS		Default
Default Windows domain		
Default Windows username		
Default Windows password		

Save

Logged on as admin since 21-Feb-2005 16:20:59
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Location Profiles

You will notice in this screen that there is a small dropdown listbox on the right hand side of the screen. Using this facility you can choose between several different 'profiles' that affect the behaviour of SSL-Explorer depending on the preferences you configure here.

Profiles are designed to allow you to configure alternative configurations depending on your location. For example, you may require the use of a proxy server at your office location but at home you have a direct internet connection. You could create two profiles, 'Home' and 'Office', with the appropriate proxy settings.

As of release 0.1.8, only the configuration options specified in this screen are stored under your profile settings.

VPN Client Options

Here you can set parameters that control the way the VPN client behaves.

- **Heartbeat interval** – The VPN client will poll the server periodically to determine whether the internet connection is still active or not. Change this value to affect the length of the interval.

- **Shutdown interval** – This is the delay between the client receiving a shutdown request and actually shutting down the VPN connection.

- **Registration Sync. Timeout** – The amount of time that the VPN client launcher will wait for the VPN client to register with the SSL-Explorer server and return successfully.

- **Start Automatically on Login** – Starts the VPN client automatically on login.

- **Browser Command** – Specifies the command that will be executed in order to launch a browser from the VPN client system tray icon (or window). Right-click on the icon to try it. This can be left blank in most situations as the client will automatically use the default browser on Windows, but is useful on Linux in cases where the client falls back to just trying to execute 'netscape'.

- **Web Forwarding Inactivity Timeout** – The amount of time to wait before closing web forwarding sessions due to inactivity.

- **Tunnel Inactivity Timeout –** The amount of time to wait before closing tunnels due to inactivity.

- **Debug** – Set this value to true to enable verbose logging to file to aid troubleshooting problems. A file sslexplorer.log will be generated in the "%USERNAME%/.sslexplorer/Applications/VPN Client" directory.

- **Proxy URL** – If you use a HTTP proxy for internet access, enter its IP address or hostname here.

- **Automatically detect proxy** – This is an experimental feature that will attempt to detect your proxy settings automatically. If you are having problems connecting to your proxy server, try disabling this feature.

Network Places

These values affect the way that the Microsoft Windows filesystem browser operates.

- **Show Hidden Files** – Toggle whether to display Windows system files in the browser.

- **Sort Folders First** – Toggle whether to display folders before files in the browser, or to sort all items regardless.

- **Sort On** – Choose which field to apply the sorting. Available options are name, size and date.

- **Reverse Sorted** – Reverses the direction of the sort.

- **Case Sensitive Sort** – Toggle whether to take case into account when sorting.

User Interface

These options affect the behaviour of the user interface:

- **CSS Location** – Specifies the location of the Cascading Style Sheet (CSS) file that is used by the web browser to render the application.

Chapter

6

Networking – Microsoft Windows Filesystem Browsing

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Keyboard exercise
- 📖 Workbook review

SSL-Explorer provides two methods for direct access to your Windows shares. SSL tunnels may also be defined in the Networking section.

Remotely Browsing Your Microsoft Windows Shares

In this part of the guide we'll assume that you have installed SSL-Explorer in the Microsoft Windows domain environment as described in the Windows installation tutorial. Instructions on configuring filesystem access for non-domain environments are coming soon.

SSL-Explorer provides Microsoft Windows filesystem browsing without the need to launch the VPN client

SSL-Explorer provides two ways to access your Microsoft Windows shared folders.

- **Web Browser** – This method of access is the easiest to setup, requiring no additional configuration by the user. Once SSL-Explorer's Active Directory configuration screen has been correctly set up, the user will have access to their home folder, and the Windows network neighbourhood.

- **Microsoft WebFolders** – Using a feature provided with Windows XP, a user can set up links to shared folders through the Add Network Place feature in Windows. These folders are browsable through Windows Explorer just like any other directory on the network, and they do not need to be recreated upon login.

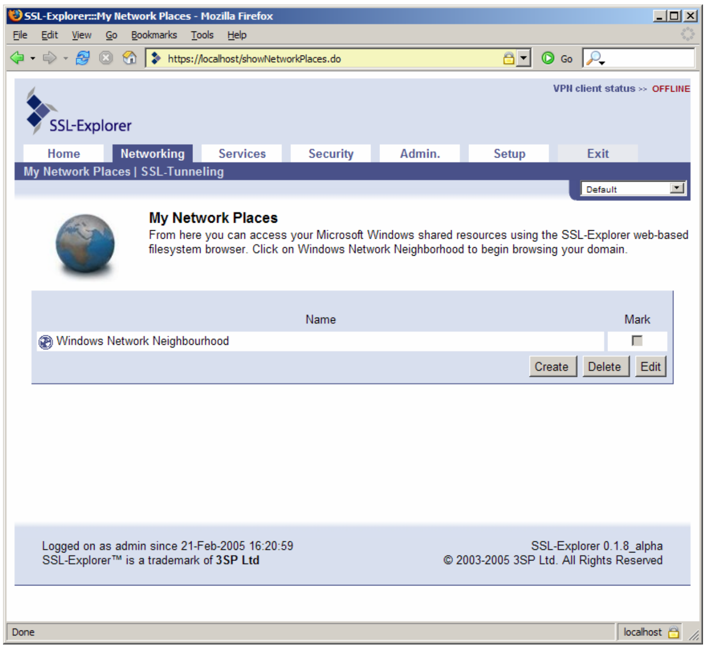
Let's take a tour of these features in more detail.

Web-Based Filesystem Browser

SSL-Explorer's web-based filesystem browser is the quickest way to retrieve say, the spreadsheet on your desktop that you forgot to make a copy of in the rush to get on that flight. The lightweight interface makes browsing a quick and painless exercise even with low bandwidth connections.

Log in to your SSL-Explorer using your Active Directory credentials and click on the networking tab at the top of the screen. Click on the subheading, 'Network Places'.

You should be presented with a screen like the following:


SSL-Explorer::My Network Places - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showNetworkPlaces.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
My Network Places | SSL-Tunneling
Default
Create
Delete
Edit
Done
localhost

My Network Places

From here you can access your Microsoft Windows shared resources using the SSL-Explorer web-based filesystem browser. Click on Windows Network Neighborhood to begin browsing your domain.

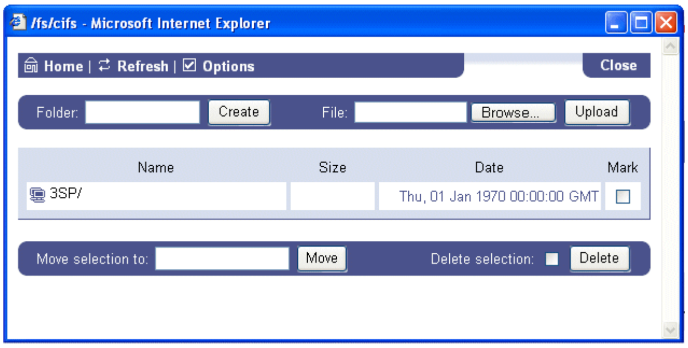
Name	Mark
Windows Network Neighbourhood	□

Logged on as admin since 21-Feb-2005 16:20:59
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

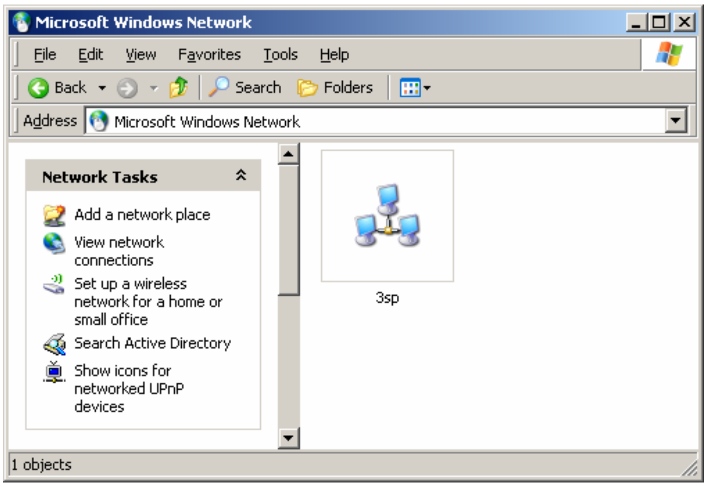
SSL-Explorer presents you with two links. The first of which is a link that will take you to your Windows home folder that was set up by your administrator.

Click on "Windows Network Neighbourhood". The filesystem browser now loads and presents you with a screen similar to the following:



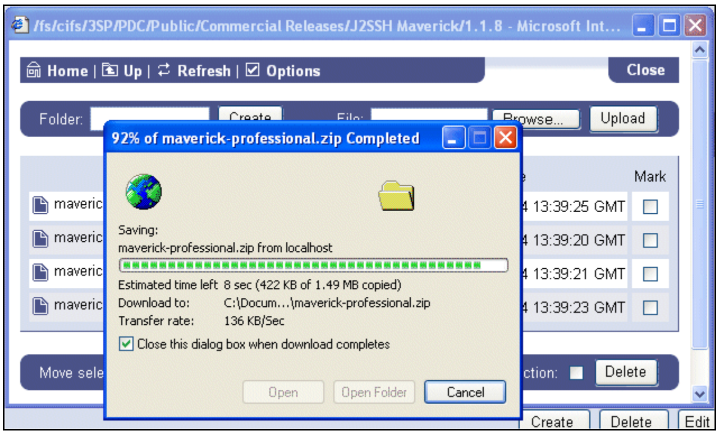
Name	Size	Date	Mark
3SP/		Thu, 01 Jan 1970 00:00:00 GMT	□

The filesystem browser displays a top-level view of the available domains that were found on the network. This view is equivalent to opening "Microsoft Windows Network" in Windows Explorer when physically inside the network, as shown in the picture below.


Microsoft Windows Network
File Edit View Favorites Tools Help
Back Search Folders
Address Microsoft Windows Network
Network Tasks
Add a network place
View network connections
Set up a wireless network for a home or small office
Search Active Directory
Show icons for networked UPnP devices
3sp
1 objects

Clicking on your domain will open the domain browser which will return a list of active systems which you may browse for resources.

Now try browsing to your previously created share on your office desktop PC and downloading a few files. Take the time to get a feel for managing files and folders with the interface.



Saving:
maverick-professional.zip from localhost

Estimated time left 8 sec (422 KB of 1.49 MB copied)
Download to: C:\Docum...\maverick-professional.zip
Transfer rate: 136 KB/Sec

☑ Close this dialog box when download completes

Web-Based Browsing

This form of filesystem access is quick and convenient but not really suitable for heavy duty remote working. For example, you cannot download multiple files at once. A better option in these cases is to set up permanent WebFolders to your often used shares in Windows XP. This way you don't even have to use a web browser to get access to your files. This method is covered next.

Browsing Shares in Windows Explorer using WebDAV and Microsoft WebFolders

Windows XP provides an easy-to-use wizard that allows you to create shortcuts to network places, and this utilizes a feature known as WebDAV. There is a WebDAV client in Windows XP and this is known as WebFolders.

What is WebDAV?

WebDAV stands for "Web-based Distributed Authoring and Versioning". It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers.

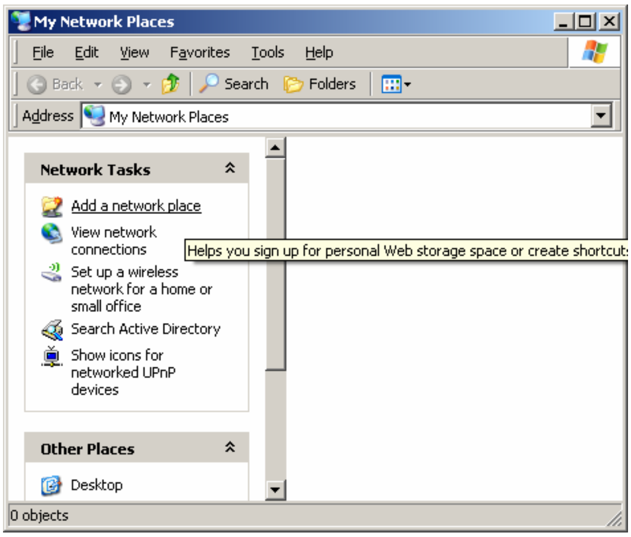
The SSL-Explorer server uses this along with CIFS to publish information on SMB-based networks such as Windows in a way that is compatible with WebDAV clients.

Using Microsoft WebFolders, links to WebDAV resources can be created that are treated much the same as any other shortcut on your network. You can create a shortcut to your company's software folder and drag this onto your desktop just as you can with any other shortcut.

The WebFolders Wizard

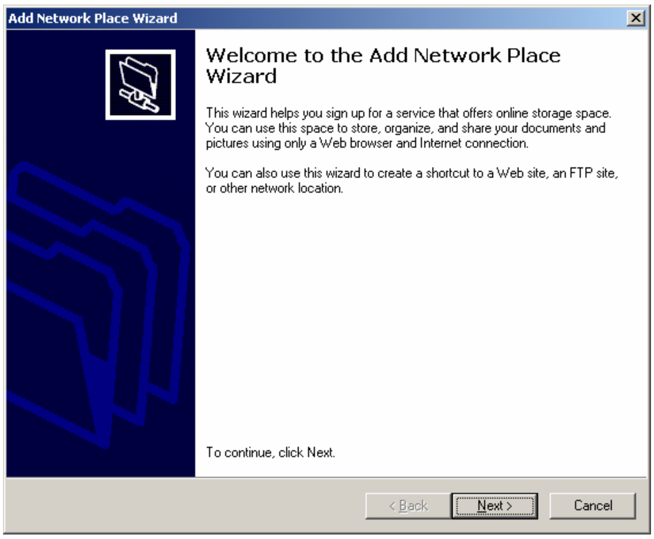
Assuming your SSL-Explorer server has already been configured with the correct information for your domain, go to your Windows desktop and double-click on "My Network Places".

Click on "Add a network place" to launch the wizard.



Helps you sign up for personal Web storage space or create shortcut:

You will be presented with the following screen. Click next.



Add Network Place Wizard

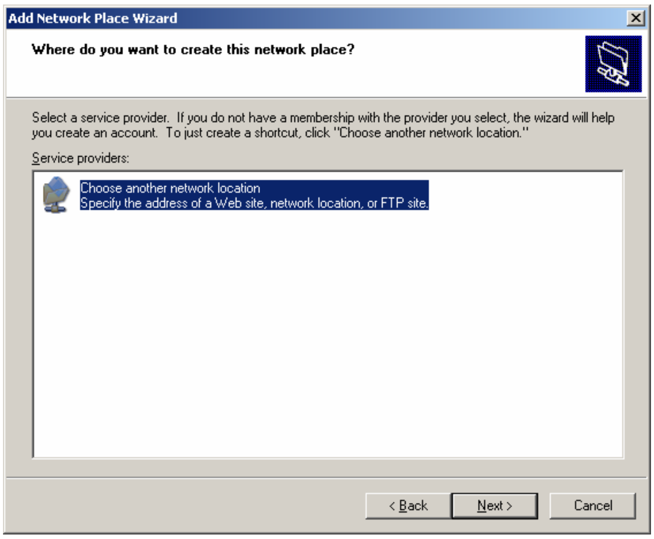
Welcome to the Add Network Place Wizard

This wizard helps you sign up for a service that offers online storage space. You can use this space to store, organize, and share your documents and pictures using only a Web browser and Internet connection.

You can also use this wizard to create a shortcut to a Web site, an FTP site, or other network location.

To continue, click Next.

The wizard will briefly search for information about service providers and will then present you with the following screen. Select "Choose another network location" and click next.



Add Network Place Wizard

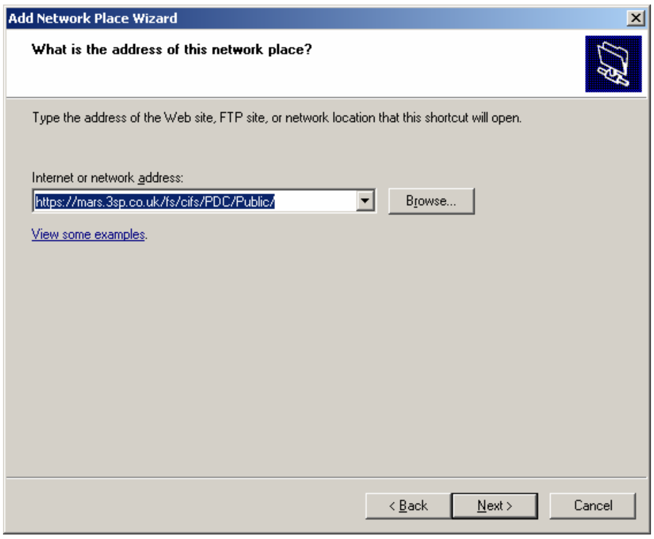
Where do you want to create this network place?

Select a service provider. If you do not have a membership with the provider you select, the wizard will help you create an account. To just create a shortcut, click "Choose another network location."

Service providers:

Choose another network location
Specify the address of a Web site, network location, or FTP site.

Now you need to enter the fully qualified domain name to your SSL-Explorer server. In our example, this is https://mars.3sp.co.uk/.



Add Network Place Wizard

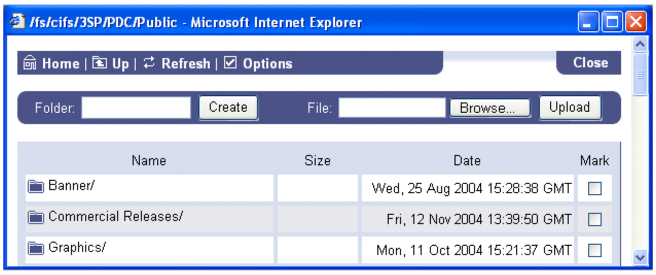
What is the address of this network place?

Type the address of the Web site, FTP site, or network location that this shortcut will open.

Internet or network address: https://mars.3sp.co.uk/fs/cifs/PDC/Public/

You also need to know the path to the resource that you want to access. An easy way of finding this out is to use the SSL-Explorer Web-based filesystem browser to locate the folder that you require and to make a note of the path shown in the title bar.

Note that in the picture below, the path is "fs/cifs/3SP/PDC/Public".



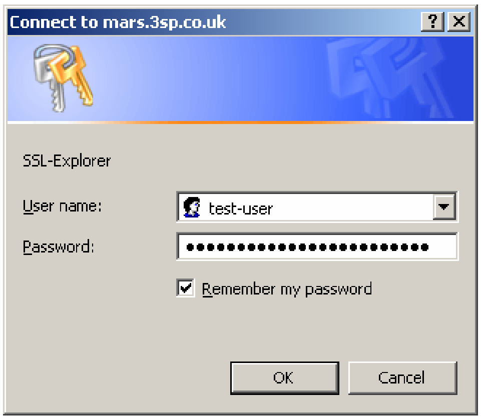
/fs/cifs/3SP/PDC/Public - Microsoft Internet Explorer

Name	Size	Date	Mark
Banner/		Wed, 25 Aug 2004 15:28:38 GMT	□
Commercial Releases/		Fri, 12 Nov 2004 13:39:50 GMT	□
Graphics/		Mon, 11 Oct 2004 15:21:37 GMT	□

Add this path onto the FQDN of your SSL-Explorer server (as above). Then click next

The WebFolders client will attempt to connect to the resource and you will be prompted to enter your Microsoft Windows account information.

Selecting "Remember my password" will store your account details in memory for the duration of your session meaning that you do not need to re-enter these each time you access the resource.


Connect to mars.3sp.co.uk

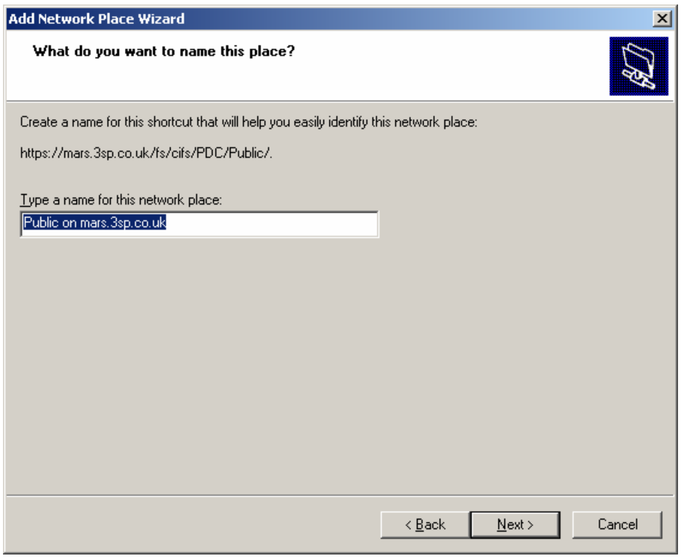
SSL-Explorer

User name: test-user

Password: ••••••••••••••••••••••••

☑ Remember my password

After successful authentication, type in a name to associate with your network place.


Add Network Place Wizard

What do you want to name this place?

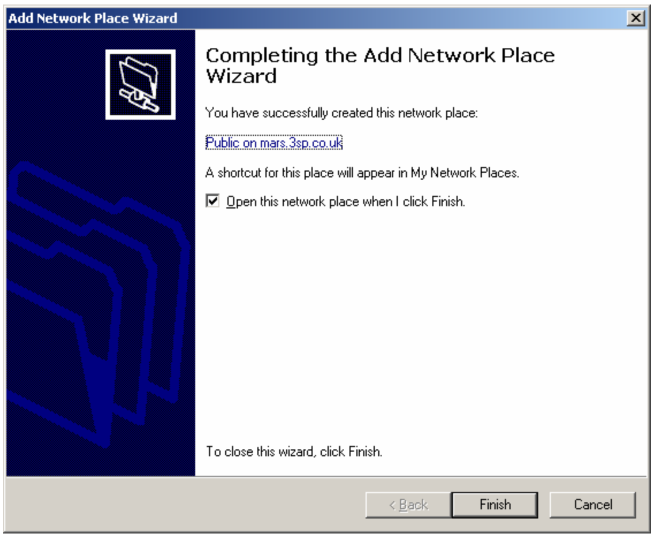
Create a name for this shortcut that will help you easily identify this network place:

https://mars.3sp.co.uk/fs/cifs/PDC/Public/.

Type a name for this network place:

Public on mars.3sp.co.uk

Congratulations. You have set up a WebFolder. Click finish to open it.



Add Network Place Wizard

Completing the Add Network Place Wizard

You have successfully created this network place:

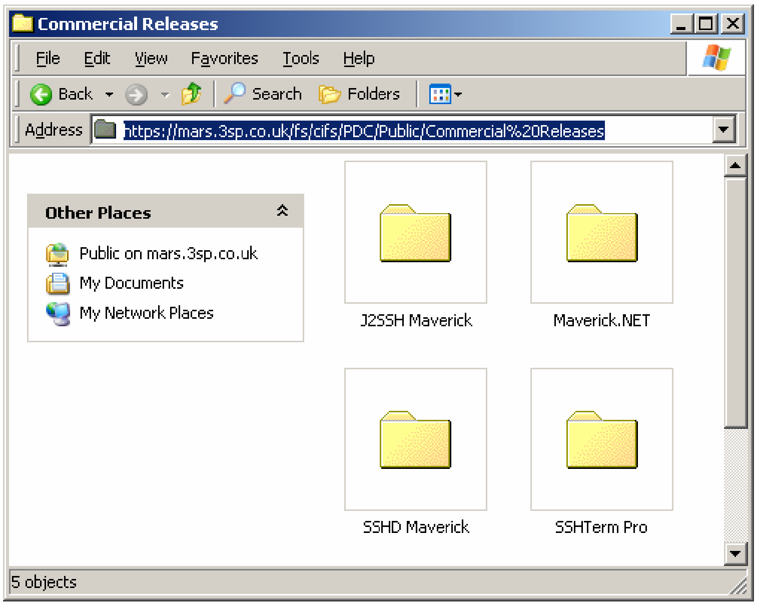
Public on mars.3sp.co.uk

A shortcut for this place will appear in My Network Places.

☑ Open this network place when I click Finish.

To close this wizard, click Finish.

Windows Explorer now opens and searches for resources. You may be asked to accept a certificate as part of the process – this is normal and ensures that your data is encrypted across the wire using SSL. You'll be prompted with a window like the one below.



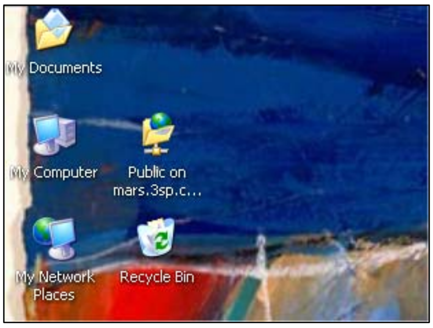
Commercial Releases

Address https://mars.3sp.co.uk/fs/cifs/PDC/Public/Commercial%20Releases

5 objects

Now drag the shortcut to your desktop if you like. From now on, all you need to do to access your shared folder is to double-click this icon and enter your Windows logon information if you haven't already.

Summary



WebFolders are a great tool for remote working and once set up is rather easy for novice users to get the hang of. After all it's just a case of clicking on an icon and entering a Windows username and password when prompted.

Anyone who has despaired whilst attempting to retrieve files from a remote computer using a cryptic combination of SSH port forwarding and Terminal Services will love the simplicity of this feature.

Similarly, our web-based filesystem browser is great for ad-hoc access to your network where the full features of WebFolders are not required. We're working on ways to extend the scope of the file browser to other filesystems and no doubt you'll be hearing more about these soon.

Remember that with SSL-Explorer acting as the proxy into your corporate network, all data across the wire is encrypted using 128-bit SSL.

Security Advisory

It should be noted that although the data is secure while in transmission, you should educate your users about leaving sensitive data on third-party computers after download. Most web browsers cache downloaded data and you should bear this in mind if your users require access to resources from borrowed PCs or internet café terminals. We are currently investigating ways of extending the security offered by our solution to cached/temporary files.

Chapter

7

Networking – SSL Tunneling and the VPN Client Applet

ICON KEY

🗁 Valuable information

✎ Test your knowledge

💻 Keyboard exercise

📖 Workbook review

How to configure commonly used applications such as Microsoft Outlook for encrypted data exchange.

Securing the insecure…

Many commonly used applications from email clients to CVS clients typically operate using unsecured protocols to facilitate the exchange of data. To the casual home user this is usually not a worry, though to the corporate user this is a critical vulnerability and one that leaves a business open to all manner of threats from password sniffing to full-blown industrial espionage.

It is not prudent to consider installing a security solution onto a Windows system without first ensuring that the system is firstly up-to-date with all published service packs and hot-fixes.

Thankfully with modern encryption protocols like SSL, data from these applications can be "tunnelled" inside SSL packets. In the case of SSL-Explorer, this is achieved through the use of the VPN client – a small applet that can intercept data transmitted by the insecure application, encrypting said data and transmitting the secure form over the wire. At the receiving end the SSL-Explorer server decrypts this data and forwards it to the appropriate destination within the trusted network.

With SSL-Explorer, you have the ability to lock down your network, leaving just a single port open on your firewall. Most traffic that would normally operate on other ports can be tunnelled through the HTTPS port 443 into your network.

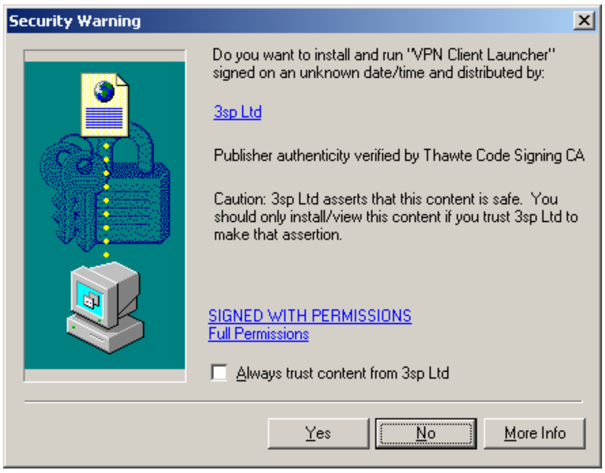
Here we will examine with real world examples how this process works.

The VPN Client

With SSL Explorer comes a small VPN client. This client is a Java application that works in conjunction with your SSL-Explorer session to provide SSL-tunneling and application launching facilities provided by the VPN server.

The client is launched by a small Java applet placed on all pages that require access to the VPN client. You only need to launch the client once per SSL-Explorer session.

Depending upon the Java Runtime Environment installed you will be prompted to trust the content of the applet. Select *yes* to ensure that the applet is loaded. The applet is signed by the developers of SSL-Explorer who assure you that the content is safe and does not represent a risk to your system, nor will it compromise your privacy.


Security Warning

Do you want to install and run "VPN Client Launcher" signed on an unknown date/time and distributed by:

3sp Ltd

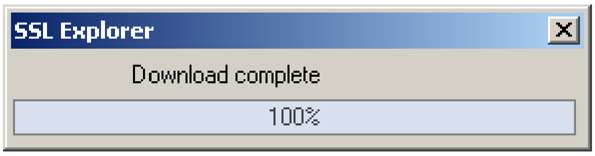
Publisher authenticity verified by Thawte Code Signing CA

Caution: 3sp Ltd asserts that this content is safe. You should only install/view this content if you trust 3sp Ltd to make that assertion.

SIGNED WITH PERMISSIONS
Full Permissions

□ Always trust content from 3sp Ltd

Once the applet has loaded you can launch the client by clicking on the “Launch” button. A dialog will display showing the progress of the download and installation.


SSL Explorer

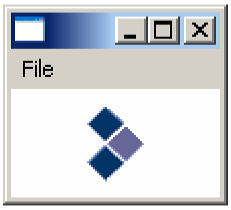
Download complete

100%

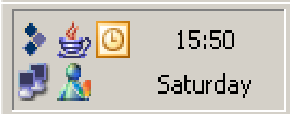
How the VPN client communicates with your browser

Some users have noticed that the VPN client listens to a number of ports in the 65500+ range. This is normal behavior. The VPN client is actually also a HTTP server and uses these ports to communicate with your web browser. All outbound network communications are sent through the HTTPS port – port 443.

Once the installation is complete the VPN client will be started. If you are using a Linux client or your browser is using either the Microsoft Java Virtual Machine or a version of the Sun Java Plug-in less than 1.2, an additional window will open to show the status of the VPN client.



For those users on Windows systems with version 1.2 or above of the Sun Java Plug-in, you will see an additional icon in the system tray which also shows the status of the VPN client.



Now that the client has started you can return back to the browser to start using the SSL tunneling and application launching features. To close the VPN client select the "Exit" link from the SSL-Explorer browser window.

Security Precautions with the VPN Client

It is important to remember that the VPN client will provide a secure tunnel into your network until it is closed or times out due to inactivity. Your users must make sure that they log-off from their SSL-Explorer sessions. It is not wise to allow such a session to remain open and unattended even for a short period of time. As of revision 0.1.7, the VPN client will timeout any tunnel that is inactive for a configurable period of time.

Securing Your POP/SMTP E-Mail Client

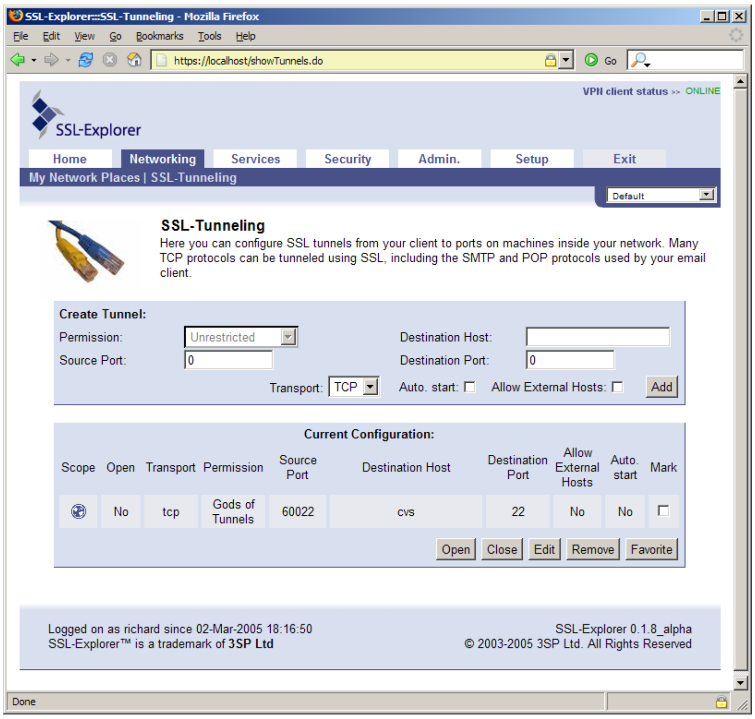
Now that you have started the VPN client you can start to take advantage of the application securing features available through SSL-tunneling (also known as port forwarding). With SSL-Explorer you have the ability to secure your existing application's communications by encrypting them and passing them through the SSL-Explorer server into your network.

Normally when you connect to your mail server using the POP protocol, your application will create a connection to port 110 and begin the exchange of email. This communication is not secure by default, but by configuring SSL Explorer you can ensure that this exchange takes place over the SSL communications channel and hence is encrypted. Many other applications can also be tunneled over SSL, for example the telnet protocol and standard HTTP web traffic.

This process is very similar to SSH forwarding but is a more flexible approach since the SSL port (port 443) is usually open on most firewalls and as such requires no additional configuration on your firewall.

Assuming the VPN client has already started, follow these steps to set up a secure tunnel for the POP protocol.

Click on the *Networking* tab and you will be presented with the port forwarding page. Here we will enter the details of the port that you wish to forward through the SSL tunnel.


SSL-Explorer::SSL-Tunneling - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showTunnels.do
Go
VPN client status >> ONLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
My Network Places | SSL-Tunneling
Default
Add
Open Close Edit Remove Favorite
Done

SSL-Tunneling

Here you can configure SSL tunnels from your client to ports on machines inside your network. Many TCP protocols can be tunneled using SSL, including the SMTP and POP protocols used by your email client.

Create Tunnel:

Permission: Unrestricted
Source Port: 0
Destination Host:
Destination Port: 0
Transport: TCP Auto. start: □ Allow External Hosts: □

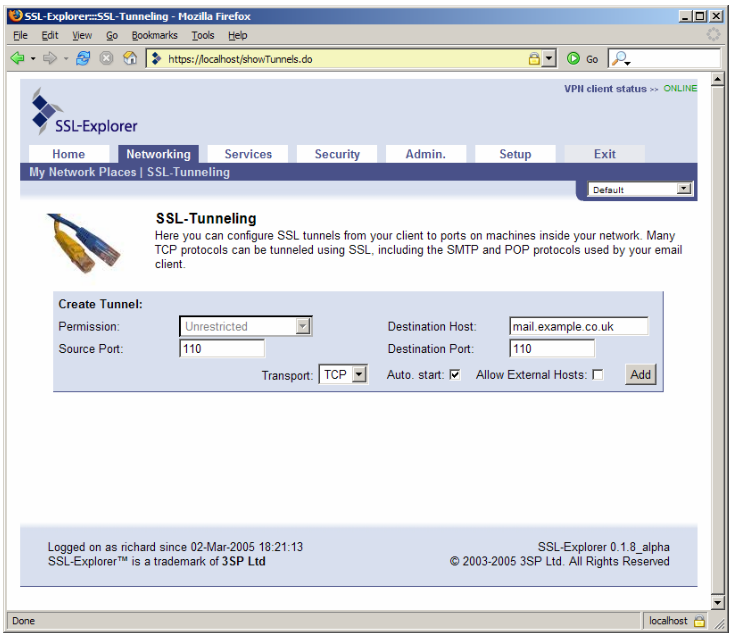
Current Configuration:

Scope	Open	Transport	Permission	Source Port	Destination Host	Destination Port	Allow External Hosts	Auto. start	Mark
⊕	No	tcp	Gods of Tunnels	60022	cvs	22	No	No	□

Logged on as richard since 02-Mar-2005 18:16:50
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Enter the details of the POP port and your mail server hostname into the fields as follows. The "allow external hosts" checkbox specifies whether you want to activate the tunnel on your current workstation only, or allow access to the tunnel from any other workstation you may log in from.


SSL-Explorer::SSL-Tunneling - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showTunnels.do
Go
VPN client status >> ONLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
My Network Places | SSL-Tunneling
Default
Add
Done
localhost

SSL-Tunneling

Here you can configure SSL tunnels from your client to ports on machines inside your network. Many TCP protocols can be tunneled using SSL, including the SMTP and POP protocols used by your email client.

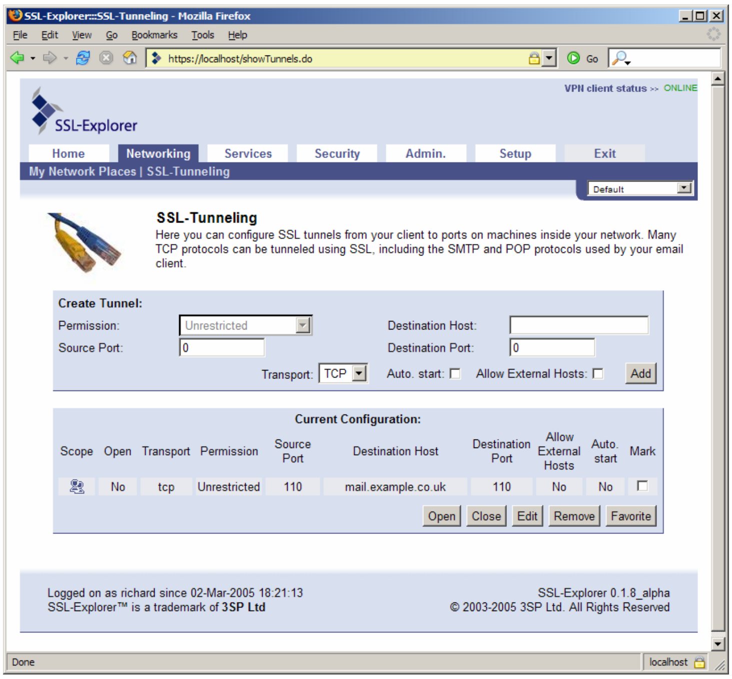
Create Tunnel:

Permission: Unrestricted
Source Port: 110
Destination Host: mail.example.co.uk
Destination Port: 110
Transport: TCP
Auto. start: ☑
Allow External Hosts: ☐

Logged on as richard since 02-Mar-2005 18:21:13
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

The tunnel will be set up and activated upon clicking add. You should see a screen similar to the following.


SSL-Explorer::SSL-Tunneling - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showTunnels.do
Go
VPN client status >> ONLINE
SSL-Explorer
Home Networking Services Security Admin. Setup Exit
My Network Places | SSL-Tunneling
Default
Add
Open Close Edit Remove Favorite
Done
localhost

SSL-Tunneling

Here you can configure SSL tunnels from your client to ports on machines inside your network. Many TCP protocols can be tunneled using SSL, including the SMTP and POP protocols used by your email client.

Create Tunnel:

Permission: Unrestricted
Source Port: 0
Destination Host:
Destination Port: 0
Transport: TCP
Auto. start: ☐
Allow External Hosts: ☐

Current Configuration:

Scope	Open	Transport	Permission	Source Port	Destination Host	Destination Port	Allow External Hosts	Auto. start	Mark
	No	tcp	Unrestricted	110	mail.example.co.uk	110	No	No	☐

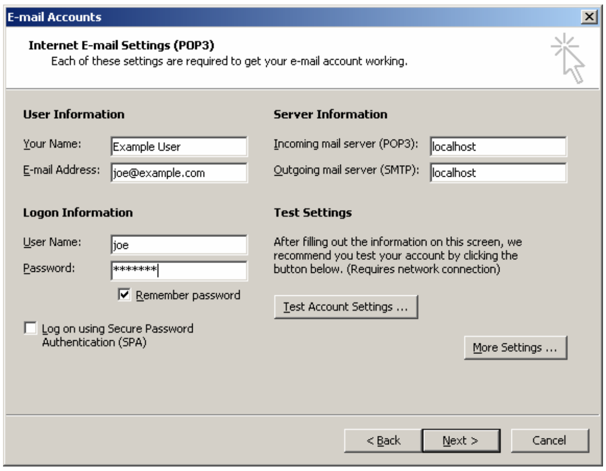
Logged on as richard since 02-Mar-2005 18:21:13
SSL-Explorer™ is a trademark of **3SP Ltd**

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

The tunnel is now configured for use with your email client. We now need to change the host setting for your mailserver. Your mail server setting is usually something similar to "*pop.example.com*". We now need to change this to "*localhost*" so that the VPN client can intercept the traffic and forward it to the SSL Explorer managed network.

For full email access, you will need to repeat this process for the SMTP protocol on port 25.

In your email client, locate your internet mail server properties and change it to something similar to the following:



Internet E-mail Settings (POP3)
Each of these settings are required to get your e-mail account working.

User Information
Your Name: Example User
E-mail Address: joe@example.com

Server Information
Incoming mail server (POP3): localhost
Outgoing mail server (SMTP): localhost

Logon Information
User Name: joe
Password: *******
☑ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

Chapter

8

Services – Remotely Accessing your Intranet Web Resources

Set up secure access to internal web servers for your users, suppliers or extranet partners.

ICON KEY

🗀	Valuable information
✎	Test your knowledge
💻	Keyboard exercise
📖	Workbook review

Secure access to the corporate intranet

On a conventional network, accessing intranet-based resources is not as straightforward as one might think. Intranet resources are not designed to be externally accessible – hence the name – and are not resolvable using the DNS system.

By using SSL-Explorer you can provide secure access to intranet applications that your remote users would not normally have access to

One way of accessing an intranet web site would be to connect to a server within the corporate network and creating a secure tunnel to the web server using something like SSH or SSL. This will of course require that an SSH server or similar is already installed on the remote PC.

Obviously, this is not a task for the uninitiated.

With SSL-Explorer, an administrator can publish links to intranet resources for access through the Web Forwards facility available under the Services tab. There are two ways to achieve this end result and these are known as the following:

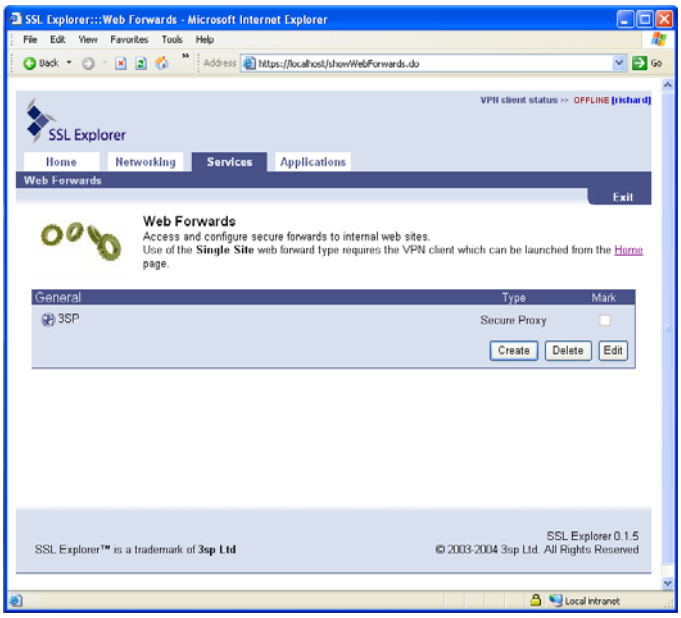
- **Single-Site Proxy** – The single site proxy requires the use of the VPN client to forward data using the tunnelling process outlined above. This feature is designed as a fall-back in cases where the secure proxy method is not appropriate.

- **Secure Proxy** – The secure proxy feature does not require the VPN client. The SSL-Explorer server actually retrieves the web page on behalf of the connecting client, replacing all links within the page to point back to the SSL-Explorer server which will repeat this process when the user requests a new page.

Web Forwarding using the Single-Site Proxy

To configure a web forward in SSL-Explorer to use the single-site proxy method, do the following:

Log into SSL-Explorer and click on the Services tab. You'll be presented with the following screen:


SSL Explorer:::Web Forwards - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForwards.do
Go
VPN client status >> OFFLINE [richard]
SSL Explorer
Home
Networking
Services
Applications
Web Forwards
Exit

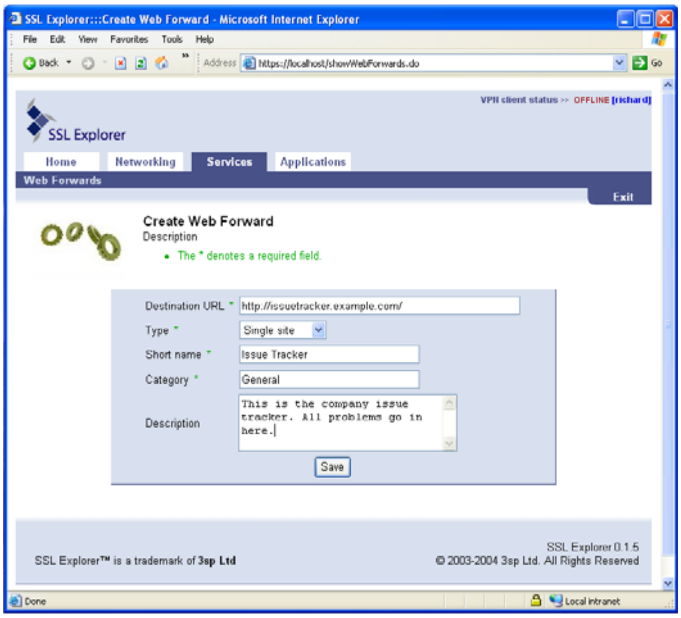
Web Forwards

Access and configure secure forwards to internal web sites.
Use of the **Single Site** web forward type requires the VPN client which can be launched from the Home page.

General	Type	Mark
3SP	Secure Proxy	□

Create
Delete
Edit
SSL Explorer™ is a trademark of 3sp Ltd
SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved
Local intranet

Click "create" to set up a new web forward. Enter the URL to the intranet resource exactly as you would if you were accessing it internally. Give the forward a name and optionally, enter a description.


SSL Explorer:::Create Web Forward - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForwards.do
Go
VPN client status >> OFFLINE [richard]
SSL Explorer
Home
Networking
Services
Applications
Web Forwards
Exit

Create Web Forward

Description

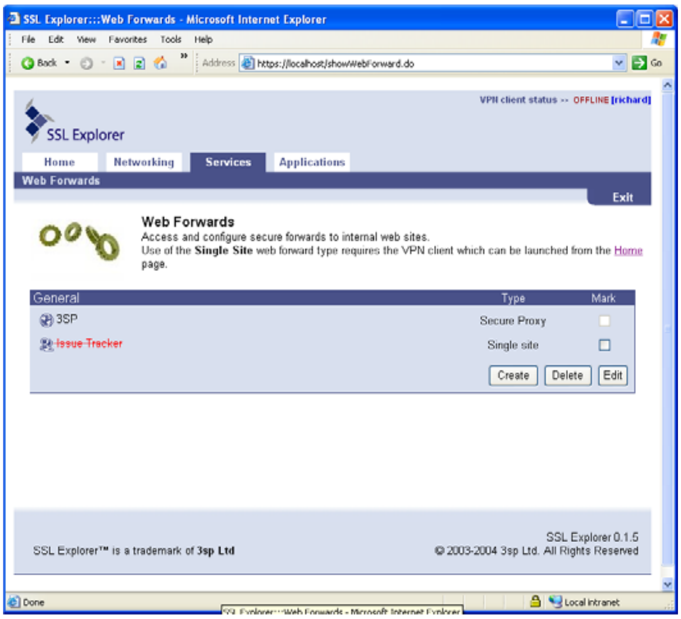
- The * denotes a required field.

Destination URL *	http://issuetracker.example.com/
Type *	Single site
Short name *	Issue Tracker
Category *	General
Description	This is the company issue tracker. All problems go in here.

Save
SSL Explorer™ is a trademark of 3sp Ltd
SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved
Done
Local intranet

Click Save.

You will be returned to the main Web Forwards page where you will be able to see your new web forward entry. Since the single-site web forwarding method requires the use of the VPN client, the entry appears in red with a strike through the name.


SSL Explorer:::Web Forwards - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForward.do
Go
VPN client status -- OFFLINE [richard]
SSL Explorer
Home
Networking
Services
Applications
Web Forwards
Exit
Create
Delete
Edit
Done
Local intranet

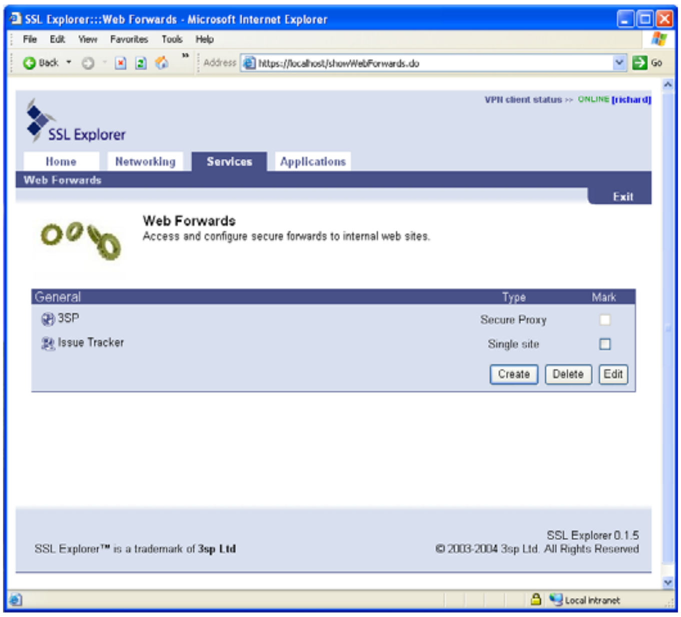
Web Forwards
Access and configure secure forwards to internal web sites.
Use of the **Single Site** web forward type requires the VPN client which can be launched from the Home page.

General	Type	Mark
3SP	Secure Proxy	□
~~Issue Tracker~~	Single site	□

SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved

Go to the home page and launch the VPN client. Then return to the Web Forwards page where you will now be able to launch the web forward. Click on its icon to spawn a browser which will connect to the intranet resource via the VPN client.


SSL Explorer:::Web Forwards - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForwards.do
Go
VPN client status -- ONLINE [richard]
SSL Explorer
Home
Networking
Services
Applications
Web Forwards
Exit
Create
Delete
Edit
Local intranet

Web Forwards
Access and configure secure forwards to internal web sites.

General	Type	Mark
3SP	Secure Proxy	□
Issue Tracker	Single site	□

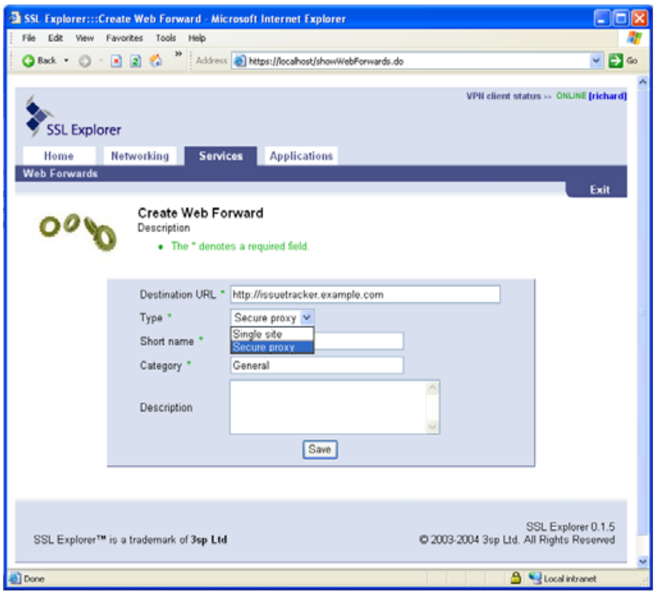
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved

Web Forwarding using the Secure Proxy

The secure proxy web forwarding is virtually identical to configure as the single-site proxy method.

When creating your web forward, select Secure Proxy from the type dropdown.


SSL Explorer:::Create Web Forward - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForwards.do
Go
VPN client status >> ONLINE [richard]
SSL Explorer
Home
Networking
Services
Applications
Web Forwards
Exit
Single site
Secure proxy
Save
SSL Explorer™ is a trademark of 3sp Ltd
SSL Explorer 0.1.5
© 2003-2004 3sp Ltd. All Rights Reserved
Done
Local intranet

Create Web Forward

Description

- The * denotes a required field.

Destination URL * http://issuetracker.example.com

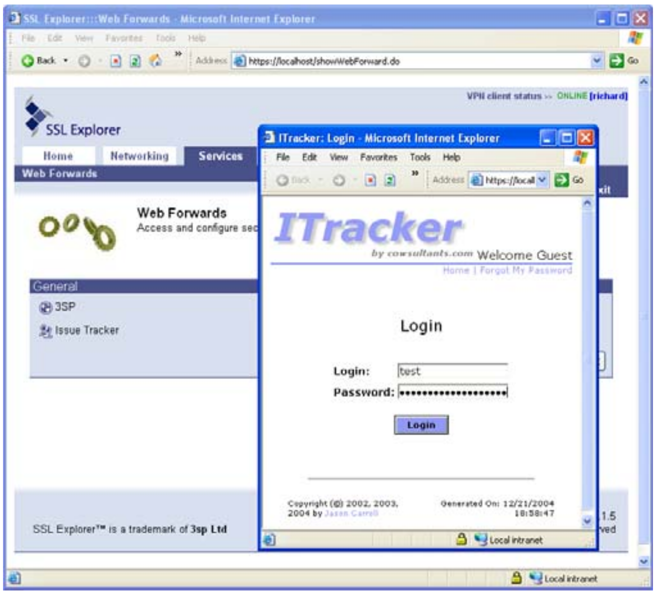
Type * Secure proxy

Short name *

Category * General

Description

Note that upon returning to the web forward page, you can access the web forward immediately, without starting the VPN client.


SSL Explorer:::Web Forwards - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://localhost/showWebForward.do
Go
VPN client status >> ONLINE [richard]
SSL Explorer
Home
Networking
Services
Web Forwards
Web Forwards
Access and configure sec
General
3SP
Issue Tracker
SSL Explorer™ is a trademark of 3sp Ltd
ITracker: Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://local
ITracker
by cowsultants.com
Welcome Guest
Home | Forgot My Password
Login
Login
Copyright (c) 2002, 2003, 2004 by Jason Carroll
Generated On: 12/21/2004 18:58:47
Local intranet

Login: test

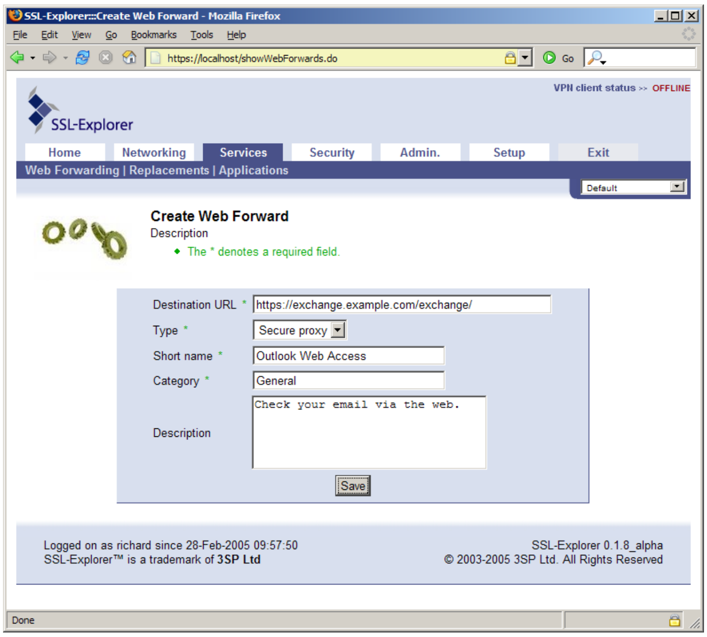
Password: ••••••••••••••••••

You can even now bookmark the link in the address bar of your intranet browser window for future use. If you are not logged into SSL-Explorer, you will be directed to the sign-in page before being granted access to the intranet resource.

Microsoft Outlook Web Access

As of release 0.1.8, SSL-Explorer supports the proxying of the Microsoft Outlook Web Access application. Please follow this process to setup a global application shortcut to the OWA application.

1. Create a new secure proxy shortcut to the OWA application running on your Exchange server.


SSL-Explorer::Create Web Forward - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showWebForwards.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Web Forwarding | Replacements | Applications
Default
Save
Done

Create Web Forward

Description

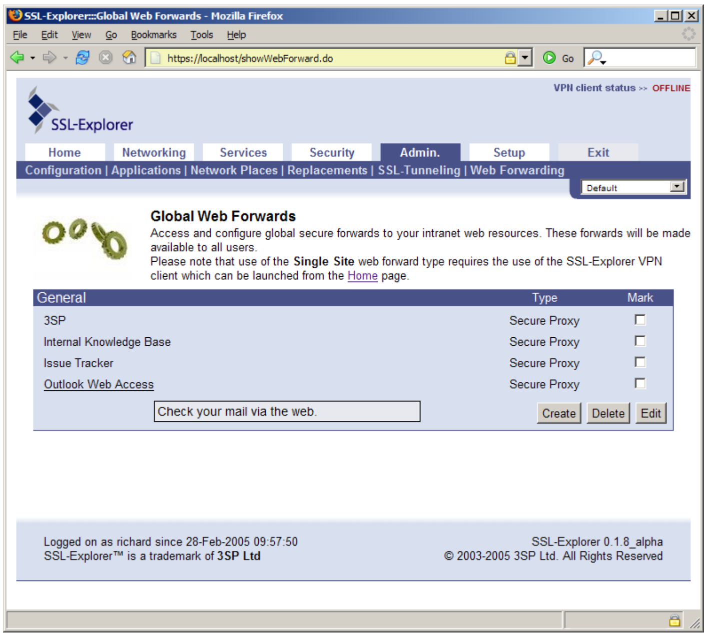
- The * denotes a required field.

Destination URL *	https://exchange.example.com/exchange/
Type *	Secure proxy
Short name *	Outlook Web Access
Category *	General
Description	Check your email via the web.

Logged on as richard since 28-Feb-2005 09:57:50
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

Your shortcut to the OWA application has been created,


SSL-Explorer::Global Web Forwards - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://localhost/showWebForward.do
Go
VPN client status >> OFFLINE
SSL-Explorer
Home
Networking
Services
Security
Admin.
Setup
Exit
Configuration | Applications | Network Places | Replacements | SSL-Tunneling | Web Forwarding
Default
Create
Delete
Edit

Global Web Forwards

Access and configure global secure forwards to your intranet web resources. These forwards will be made available to all users.

Please note that use of the **Single Site** web forward type requires the use of the SSL-Explorer VPN client which can be launched from the Home page.

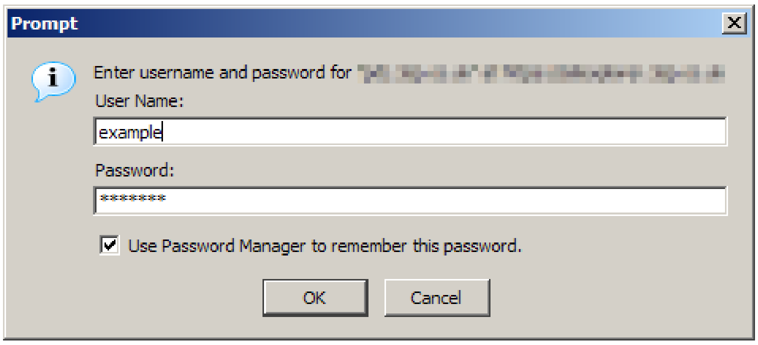
General	Type	Mark
3SP	Secure Proxy	□
Internal Knowledge Base	Secure Proxy	□
Issue Tracker	Secure Proxy	□
Outlook Web Access	Secure Proxy	□

Check your mail via the web.

Logged on as richard since 28-Feb-2005 09:57:50
SSL-Explorer™ is a trademark of 3SP Ltd

SSL-Explorer 0.1.8_alpha
© 2003-2005 3SP Ltd. All Rights Reserved

2. Click on the shortcut to launch the OWA application, which will prompt you for your Exchange username and password. This is usually the same as your Windows domain account credentials.



Prompt

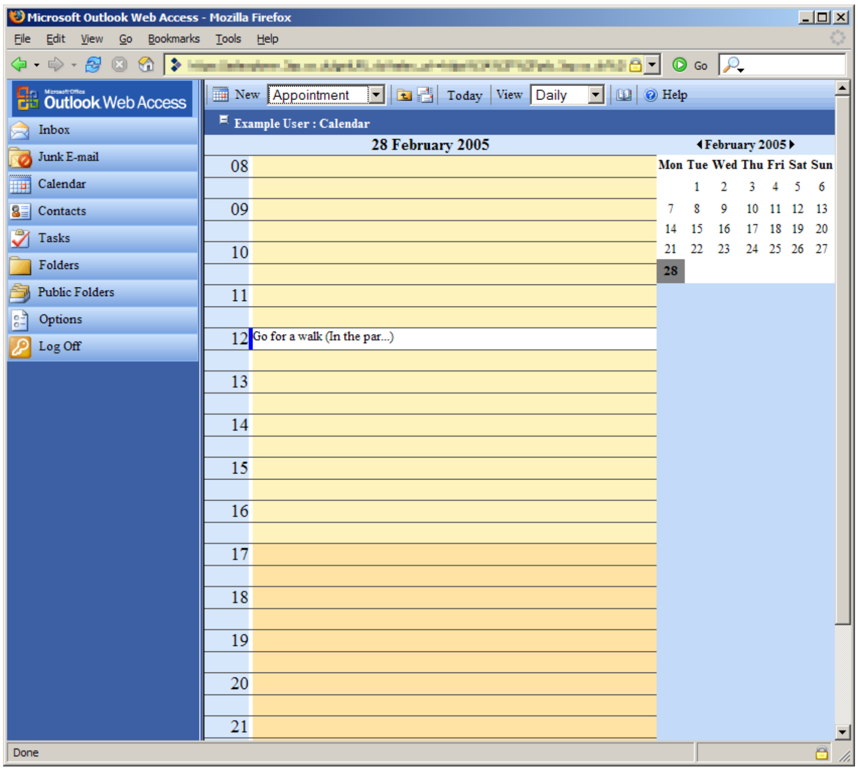
Enter username and password for [redacted]

User Name: example

Password: ********

☑ Use Password Manager to remember this password.

3. You are now connected to the Outlook Web Access application.



Microsoft Outlook Web Access - Mozilla Firefox

Example User : Calendar

28 February 2005

12 Go for a walk (In the par...)

🗁 Exchange 2003 and the OWA ActiveX Control

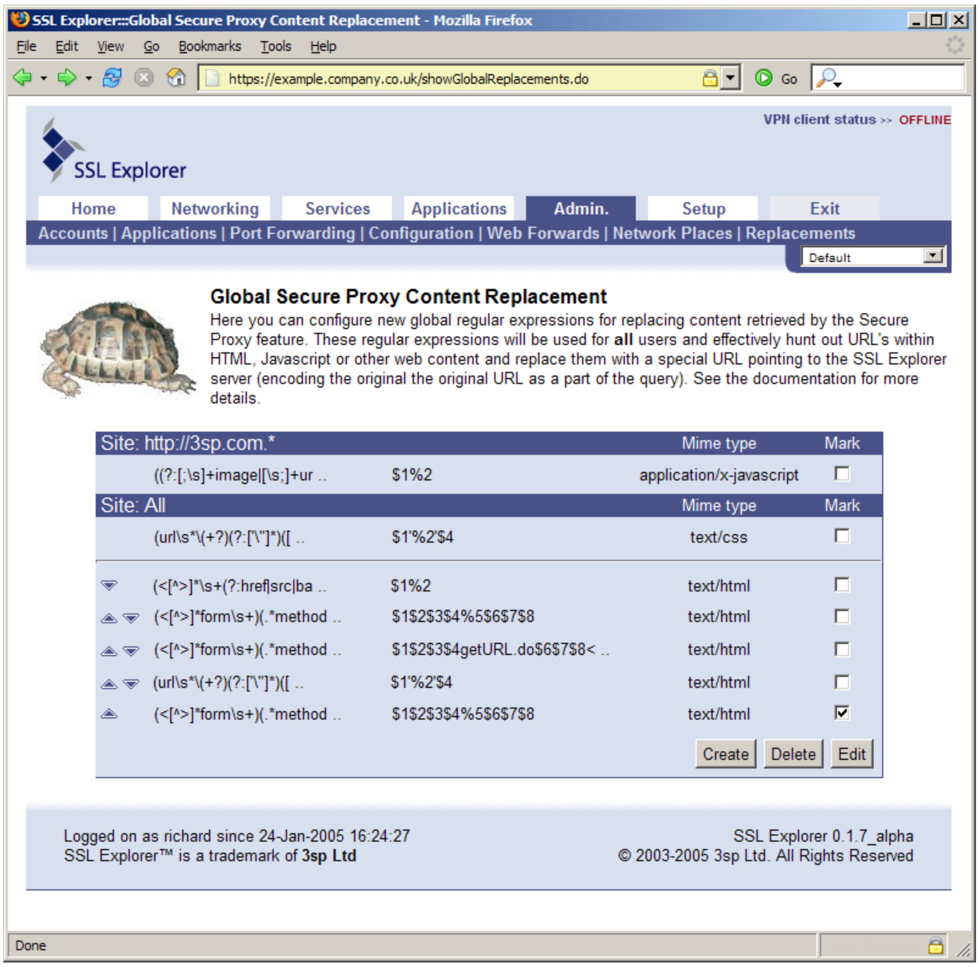
As of release 0.1.8, support for the Exchange 2003 ActiveX control has not been implemented. We are looking into ways of providing this feature in an upcoming release.

Secure Proxy Content Replacement

The secure proxy service works by transforming the paths of image sources and hyperlinks on intranet pages in such a way that requests to these resources are redirected to the SSL-Explorer server which fetches the web page on the user's behalf, again performing this transformation on the fetched page. It does this by replacing their original URLs with ones that point to the SSL-Explorer server.

This process works fine for more basic web pages, though certain intranet resources that use extensive ASP or JavaScript may prove problematic. For example, the Microsoft Exchange 2003 Outlook Web Access application will fail when proxied through SSL-Explorer versions prior to 0.1.8. This is because not all URLs are successfully matched and replaced by the current version of SSL-Explorer.

To address this problem we allow for custom content replacement values to be specified. The SSL-Explorer will locate instances of the values and replace them with a replacement value that you specify. The ultimate aim of which is to capture all rogue URLs that are not already being transformed, and replace them with custom URLs that are described in this section.


SSL Explorer:::Global Secure Proxy Content Replacement - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://example.company.co.uk/showGlobalReplacements.do
Go
VPN client status >> OFFLINE
SSL Explorer
Home Networking Services Applications Admin. Setup Exit
Accounts | Applications | Port Forwarding | Configuration | Web Forwards | Network Places | Replacements
Default
Create Delete Edit
Done

Global Secure Proxy Content Replacement

Here you can configure new global regular expressions for replacing content retrieved by the Secure Proxy feature. These regular expressions will be used for **all** users and effectively hunt out URL's within HTML, Javascript or other web content and replace them with a special URL pointing to the SSL Explorer server (encoding the original the original URL as a part of the query). See the documentation for more details.

<table>
<tr><th colspan="3">Site: http://3sp.com.*</th><th>Mime type</th><th>Mark</th></tr>
<tr><td></td><td>((?:[;\s]+image|[\s;]+ur ..</td><td>$1%2</td><td>application/x-javascript</td><td>□</td></tr>
<tr><th colspan="3">Site: All</th><th>Mime type</th><th>Mark</th></tr>
<tr><td></td><td>(url\s*\(+?)(?:['\"]*)([..</td><td>$1'%2'$4</td><td>text/css</td><td>□</td></tr>
<tr><td>▽</td><td>(<[^>]*\s+(?:href|src|ba ..</td><td>$1%2</td><td>text/html</td><td>□</td></tr>
<tr><td>△ ▽</td><td>(<[^>]*form\s+)(.*method ..</td><td>$1$2$3$4%5$6$7$8</td><td>text/html</td><td>□</td></tr>
<tr><td>△ ▽</td><td>(<[^>]*form\s+)(.*method ..</td><td>$1$2$3$4getURL.do$6$7$8< ..</td><td>text/html</td><td>□</td></tr>
<tr><td>△ ▽</td><td>(url\s*\(+?)(?:['\"]*)([..</td><td>$1'%2'$4</td><td>text/html</td><td>□</td></tr>
<tr><td>△</td><td>(<[^>]*form\s+)(.*method ..</td><td>$1$2$3$4%5$6$7$8</td><td>text/html</td><td>☑</td></tr>
</table>

Logged on as richard since 24-Jan-2005 16:24:27
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2005 3sp Ltd. All Rights Reserved

Regular Expressions and Capturing Groups

The main feature that SSL-Explorer uses for string replacement is known as 'capturing groups'. You effectively write what is known as a regular expression to break a matched string up into parts. For instance, say you want to replace the URL in an image tag such as:

```
<img src="http://www.google.com/image.gif"/>
```

You need to extract the URL part and replace only that, so you write a regular expression to break it up into its constituent parts:

```
(img src=\")([^\"])(\")
```

That breaks the URL into three capturing groups. The first one will contain:

```
img src="
```

The second will contain:

```
http://www.google.com
```

And the third:

```
"/>
```

The corresponding replacement pattern is:

```
$1%2$3
```

This is defined as:

$1 – Replace capturing group one verbatim.

%2 – Replace capturing group two with the proxied path.

$3 – Replace capturing group three verbatim.

Content replacement is an advanced feature designed for technically aware users. We're working on ways to provide greater support to allow for greater "webification" of your intranet applications. We have used the Pattern class from the 1.4.2 JDK to perform this function, and there is documentation available from Sun Microsystems[5] that you will need to refer to for a full list of the parameters available for regular expressions.

[5] http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html

Chapter 9

Services – Securing and Launching Applications

SSL-Explorer can deploy Java applications, and execute client-side native Windows applications.

ICON KEY

🗁	Valuable information
✎	Test your knowledge
💻	Keyboard exercise
📖	Workbook review

Application Deployment

Applications built using the Java programming language are cross-platform by nature. These days a whole host of Java applications are available that can be used as direct replacements for single-platform applications. The good news is that Java applications can be deployed to users over the web using SSL-Explorer.

Use SSL-Explorer to save time and money by giving your users quick and easy access to the applications they need.

To take a real world example, say that you have fifty users in your accounts department who require ad-hoc access to a number of Unix servers using SSH. Now if you are a big fan of progress bars, you could install a Windows SSH client on each of their fifty PCs (then do it all again when the next version comes out!).

Most people however tend to value their sanity, so alternatively you could publish a Java-based SSH client on your SSL-Explorer server once only, and have each user launch the SSH client from there when they need the use of it. Remember that SSL-Explorer is just as great for internal use as it is for remote access.

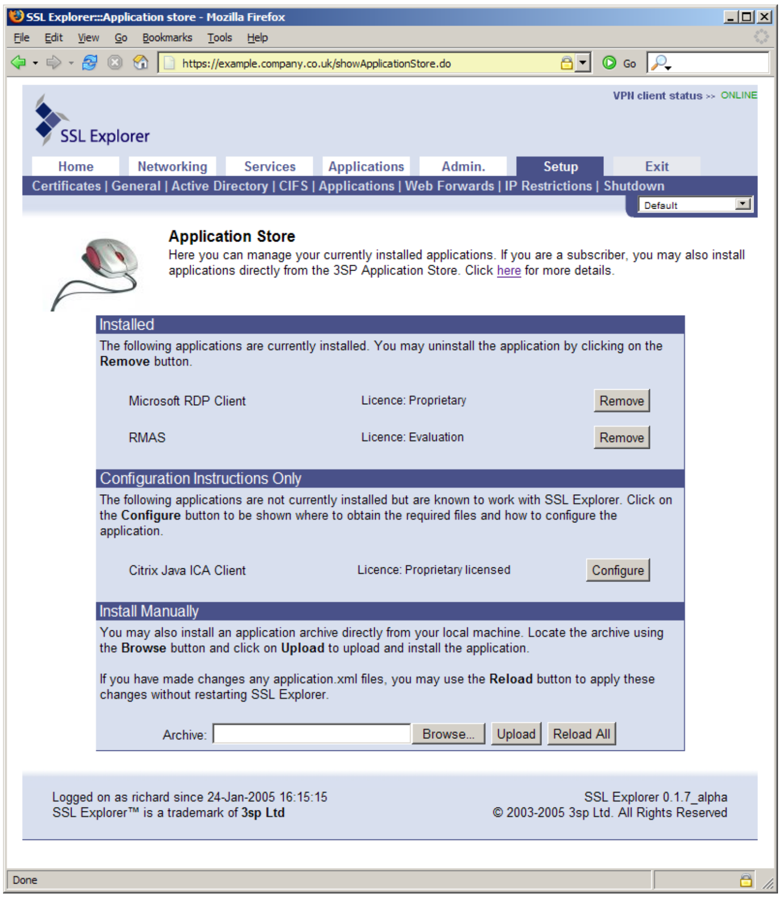
Almost any Java application (note not applet) can be published on the server in this manner. The commonly-used Java Citrix ICA client can be deployed in this manner to provide remote access to internal Citrix Metaframe servers. Examples are available that allow the deployment of the Java RDP client – ProperJavaRDP.

🗁 The 3SP Online Application Store

Now you can automatically download and install a number of applications direct from the 3SP Online Application Store within SSL-Explorer. A series of pre-configured applications/applets are available for simple one-click installation.

The 3SP Online Application Store

With the release of SSL-Explorer 0.1.7, a facility has been added to allow installation of applications over the internet. When accessing the application setup page in SSL-Explorer, your server will check with the 3SP Online Application Store to determine what applications are available for instant installation. These currently include various SSH clients, MS Terminal Services, VNC and IRC.


SSL Explorer:::Application store - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://example.company.co.uk/showApplicationStore.do
Go
VPN client status >> ONLINE
SSL Explorer
Home Networking Services Applications Admin. Setup Exit
Certificates | General | Active Directory | CIFS | Applications | Web Forwards | IP Restrictions | Shutdown
Default

Application Store

Here you can manage your currently installed applications. If you are a subscriber, you may also install applications directly from the 3SP Application Store. Click here for more details.

Installed

The following applications are currently installed. You may uninstall the application by clicking on the **Remove** button.

Microsoft RDP Client	Licence: Proprietary	Remove
RMAS	Licence: Evaluation	Remove

Configuration Instructions Only

The following applications are not currently installed but are known to work with SSL Explorer. Click on the **Configure** button to be shown where to obtain the required files and how to configure the application.

Citrix Java ICA Client	Licence: Proprietary licensed	Configure

Install Manually

You may also install an application archive directly from your local machine. Locate the archive using the **Browse** button and click on **Upload** to upload and install the application.

If you have made changes any application.xml files, you may use the **Reload** button to apply these changes without restarting SSL Explorer.

Archive: Browse... Upload Reload All

Logged on as richard since 24-Jan-2005 16:15:15
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2005 3sp Ltd. All Rights Reserved

Automatic Installation

From here, installing many applications now becomes a one-click process with the application binaries and associated configuration files simply downloaded and installed on your SSL-Explorer server. Unfortunately, not all software can be installed in this manner due to licensing incompatibilities, though most open source software may be redistributed without licensing problems.

Manual Installation

For applications whose licenses do not permit redistribution, such as the Citrix Java ICA client, you will notice a "configure" button which when clicked will direct your browser to a knowledge base article that details the installation process.

Finally, there is now also an "install manually" option. Using this method you can upload a previously prepared ZIP file containing the application binaries and your application's descriptor file, named *application.xml*.

Using XML Files for Java Application Deployment

SSL-Explorer gives the administrator the ability to deploy commonly used Java applications for quick and easy access from any Java-enabled browser. A user can simply select an application and SSL Explorer will download the necessary files and launch the application. If the application has configurable command line parameters then these can be set up as shortcuts and saved to the users profile allowing the user to log in using any Java-enabled browser and launch the application with a single click.

Deploying an application via the SSL Explorer involves creating a directory for each of your chosen applications under *$INSTALL_DIR/webapp/WEB-INF/applications*, and copying the applications program files to this location along with a descriptor file called *application.xml.*

The following XML file is an example of a simple descriptor that will deploy, launch and tunnel the popular open source remote access client, VNC. This file may be downloaded from the 3SP Knowledge Base at http://3sp.com/kb or may also be installed from the 3SP Online Application Store.

```
<application version="1.0" type="java" application="VNC"
name="Virtual Network Computing (VNC)" license="GPL"
productURL="http://www.tightvnc.com/">

    <description>VNC software makes it possible to view and
fully-interact with one computer from any other computer or
mobile device anywhere on the Internet.</description>

    <parameter type="0" sequence="0" name="hostname"/>
    <parameter type="1" sequence="1" name="port"/>

      <messages>
            <message key="hostname.name">Hostname</message>
            <message key="port.name">Port</message>
      </messages>

    <tunnel name="vnc" hostname="${shortcut:hostname}"
port="${shortcut:port}" usePreferredPort="false"/>

      <java jre="1.1">
            <classpath>
              <jar>VncViewer.jar</jar>
            </classpath>
         <main class="VncViewer">
              <arg>HOST</arg>
              <arg>${tunnel:vnc.hostname}</arg>
              <arg>PORT</arg>
              <arg>${tunnel:vnc.port}</arg>
         </main>
      </java>

</application>
```

Deploying the Citrix Java ICA Client

Citrix are a leading vendor of remote access solutions that provide access to centralised applications through the Citrix Metaframe suite of products.

Accessing Metaframe servers can be achieved through a number of ways, one of which being the Citrix Java ICA client that is freely downloadable from Citrix[6]. This client, like many Java applications, can be published on the SSL-Explorer VPN server for use by your users.

1. Firstly locate and download the 7.2 version of the ICA client from Citrix

2. Extract the contents of the ICA client distribution in to the following directory: *$SSLEXPLORER_INSTALL_DIR/webapp/WEB-INF/applications/*

3. A folder named *JICAComponents* should have been created. Please check that the path to *JICAEngJ.jar* is: *$SSLEXPLORER_INSTALL_DIR/webapp/WEB-INF/applications/JICAComponents/JICAEngJ.jar*

4. Copy the application.xml file that accompanies this knowledge base article into the *JICAComponents* folder.

5. Restart the SSL-Explorer service to load the new application

The following XML file defines how the Citrix ICA 7.2 client is launched. Please note that you cannot use the latest 8.2 client with SSL-Explorer This file may be downloaded from the 3SP Knowledge Base at http://3sp.com/kb.

```
<application version="1.0" type="java" application="JICAComponents"
name="Citrix Published Applications" jre="1.4.2" productURL="
http://www.citrix.com/site/SS/downloads/details.asp?dID=2755&amp;down
loadID=8758&amp;pID=186">

<description>Citrix published applications.</description>

<parameter name="Hostname" type="0" sequence="0"
default="MyCitrixServer"/>
<parameter name="Application" type="0" sequence="1"
default="AppName"/>
<parameter name="Screen_Width" type="3" sequence="2"
typeMeta="800,1024,1280" default="800"/>
<parameter name="Screen_Height" type="3" sequence="3"
typeMeta="600,768,1024" default="600"/>

<messages>
        <message key="Hostname.name">Hostname:</message>
        <message key="Hostname.description">Please enter the
hostname/IP of your Citrix server</message>
        <message key="Application.name">Application:</message>
        <message key="Application.description">Enter the name of your
Citrix application here</message>
```

[6] **Citrix ICA 7.2 Client Download URL:** http://www.citrix.com/site/SS/downloads/details.asp?dID=2755&downloadID=8758&pID=186

```
        <message key="Screen_Width.name">Screen Width:</message>
        <message key="Screen_Width.description">Choose your screen
width</message>
        <message key="Screen_Height.name">Screen Height:</message>
        <message key="Screen_Height.description">Choose your screen
height</message>
        <message key="Screen_Height.value.600">600</message>
        <message key="Screen_Height.value.768">768</message>
        <message key="Screen_Height.value.1024">1024</message>
        <message key="Screen_Width.value.800">800</message>
        <message key="Screen_Width.value.1024">1024</message>
        <message key="Screen_Width.value.1280">1280</message>
</messages>

<tunnel name="JICAComponents" hostname="${shortcut:Hostname}"
port="1494" usePreferredPort="true"/>

<java jre="1.1">
        <classpath>
                <jar>JICAEngJ.jar</jar>
        </classpath>

        <main class="com.citrix.JICA">
                <arg>-Address:${tunnel:JICAComponents.hostname}</arg>
                <arg>-InitialProgram:#${param:Application}</arg>
                <arg>-Height:${param:Screen_Height}</arg>
                <arg>-Width:${param:Screen_Width}</arg>
                <arg>-ShowStatusBar:no</arg>
        </main>
</java>
```

```
</application>
```

This XML file will currently not allow use of the server browsing or load-balancing features. The file does not launch the Connection Center but you can easily do so by changing the main class line to read:

```
<main class="com.citrix.ConnectionCenter">
```

Unless you need to look at or change client-side server mappings, status information or switch to full-screen mode, this is not needed.

Executing Windows Native Applications

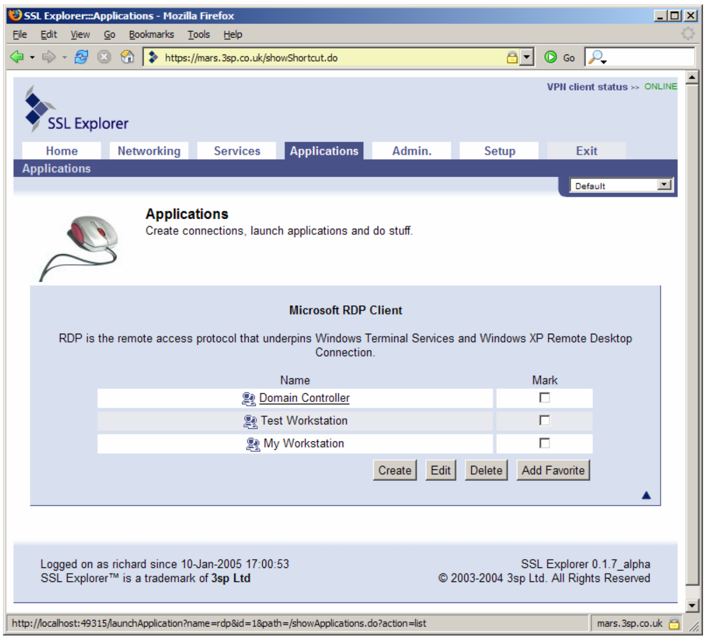
SSL-Explorer has the ability to execute any client-side application whose location resides in the Windows PATH statement. You can also pass command line arguments to your application to affect its behaviour. One example of this useful feature is the use of the Microsoft Remote Desktop client on Windows client systems as an alternative to the lesser featured Java-based RDP client.

Native Windows Remote Desktop support can be downloaded through the 3SP Online Application Store. Alternatively you may create an *application.xml* file with the following contents and install the file as detailed previously.

```
<application type="executable" application="rdp"
name="Microsoft RDP Client">

      <description>RDP is the remote access protocol that
      underpins Windows Terminal Services and Windows XP Remote
      Desktop Connection.</description>

      <parameter type="0" name="hostname" sequence="1"/>
      <parameter type="1" name="port" sequence="2"
      default="3389"/>
      <parameter type="2" name="fullScreen" sequence="3"
      default="false"/>
      <parameter type="1" name="width" sequence="4"
      default="800"/>
      <parameter type="1" name="height" sequence="5"
      default="600"/>

      <messages>
         <message key="hostname.name">Hostname</message>
         <message key="port.name">Port</message>
         <message key="fullScreen.name">Full screen</message>
         <message key="width.name">Width</message>
         <message key="height.name">Height</message>
      </messages>

      <tunnel name="rdp" usePreferredPort="false"
      hostname="${shortcut:hostname}" port="${shortcut:port}"
      width="${shortcut:width}" height="${shortcut:height}"/>

      <executable program="mstsc.exe">
         <if parameter="fullScreen" value="true">
            <arg>/f</arg>
         </if>
         <arg>/v:${tunnel:rdp.hostname}:${tunnel:rdp.port}
      /w:${param:width} /h:${param:height}</arg>
      </executable>

</application>
```

To connect to a Windows XP system using RDP, you will have to configure the host system to accept Remote Desktop Connections. You can do this in Control Panel, using the Remote tab in System Properties.

Once this is done, try creating some SSL-Explorer application shortcuts to remote systems on your network:


SSL Explorer::Applications - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://mars.3sp.co.uk/showShortcut.do
Go
SSL Explorer
Home
Networking
Services
Applications
Admin.
Setup
Exit
Default
Create
Edit
Delete
Add Favorite
mars.3sp.co.uk

VPN client status >> ONLINE

Applications

Applications

Create connections, launch applications and do stuff.

Microsoft RDP Client

RDP is the remote access protocol that underpins Windows Terminal Services and Windows XP Remote Desktop Connection.

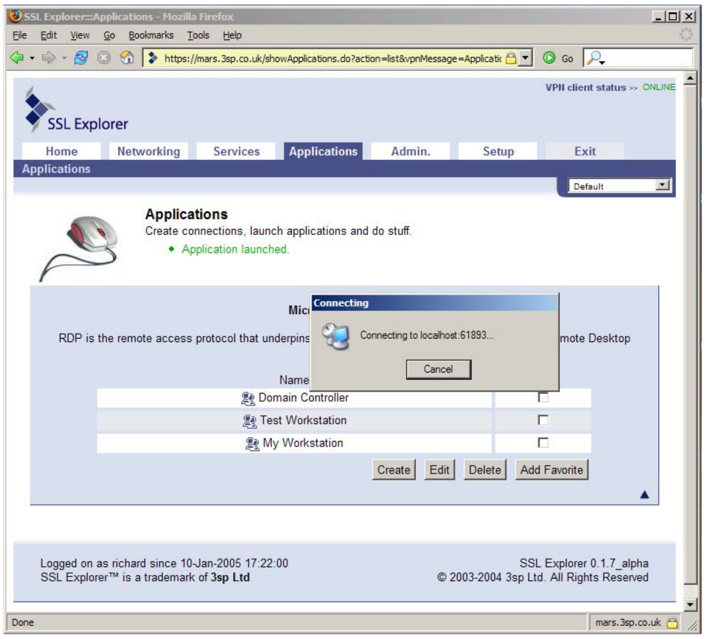
Name	Mark
Domain Controller	☐
Test Workstation	☐
My Workstation	☐

Logged on as richard since 10-Jan-2005 17:00:53
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2004 3sp Ltd. All Rights Reserved

http://localhost:49315/launchApplication?name=rdp&id=1&path=/showApplications.do?action=list

Clicking on your shortcut will spawn the native Microsoft Windows Remote Desktop client which will use the SSL-Explorer VPN client to establish an RDP session with your remote system.


SSL Explorer::Applications - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://mars.3sp.co.uk/showApplications.do?action=list&vpnMessage=Applicatio
Go
SSL Explorer
Home
Networking
Services
Applications
Admin.
Setup
Exit
Default
Connecting
Cancel
Create
Edit
Delete
Add Favorite
mars.3sp.co.uk

VPN client status >> ONLINE

Applications

Applications

Create connections, launch applications and do stuff.

- Application launched.

Mic

RDP is the remote access protocol that underpins … mote Desktop

Connecting to localhost:61893...

Name	
Domain Controller	☐
Test Workstation	☐
My Workstation	☐

Logged on as richard since 10-Jan-2005 17:22:00
SSL Explorer™ is a trademark of **3sp Ltd**

SSL Explorer 0.1.7_alpha
© 2003-2004 3sp Ltd. All Rights Reserved

Done

Creating Your Own Application XML Files

We have created several example *application.xml* files for popular applications, though there may be instances where you wish to deploy an unsupported application on the SSL-Explorer VPN. This is an in-depth guide to the available elements and properties that are available to create your own XML file.

The <application> Element

This root element requires the following attributes:

Attribute	What it Means	Required?
application	This is a unique name/ID for the application.	Yes
name	The application name that you wish to be displayed to the user on the SSL Explorer Applications page.	Yes
Type	This attribute indicates the type of application. Currently, the supported types are:- • ***Executable* -** Native application launching. • ***Java* -** Java application launching. • ***Html* -** Applet and ActiveX launching.	Yes
version	This is the version (in major.minor format) of the application descriptor, not the actual applications version. It should match the version in the 3SP Application Store descriptor (if the application is in the store of course).	Yes
jre	The minimum version of Java for which the application is built. When attempting to launch an application, the SSL Explorer VPN client will not launch the application if the installed Java runtime environment is lower that this value. This attribute will accept values in the format "1.1", "1.2", "1.3", "1.4" and also "1.3.1", "1.4.2" etc.	Yes
License	Some text to give information about the license type of the application e.g. "GPL",	No

	“Proprietary”.	
productURL	The URL to the application’s product page. Enter the URL of the product page/company website here.	No

The <parameter> Element

A parameter is presented to the user when they create a shortcut for the application. Any values entered by the user are stored and when an application is launched the VPN client will replace any instances of the parameter found in the *application.xml* file with the value entered by the user.

You can define a parameter using the following element

```
<parameter type="0" sequence="0" name="hostname"/>
<parameter type="1" sequence="1" name="port"
default="22"/>
```

These parameters can be accessed later in the descriptor by using the string replacement facility which we will come to later.

An example of how to use parameters can be seen in the VNC example:

```
<tunnel name="vnc" hostname="${shortcut:hostname}"
port="${shortcut:port}" usePreferredPort="false"/>
```

Attribute	What it Means	Required?
Name	A unique name for the parameter e.g. “Hostname”.	Yes
Type	This determines how the parameter will be presented to the user when they are creating shortcuts. It may be one of:- 0. Text 1. Number 2. Check-box 3. Menu 4. Password 5. Editable list	Yes

	6. Text area	
Sequence	Determines the order in which the parameter will appear.	Yes
typeMeta	Some types may specify meta data. If the type is either 5 or 6, you may specify the size of the text area that is displayed by setting a value of "<columns>x<rows>". If the type is 3, then you may supply a list of values, e.g. "on,off,auto".	No
Hidden	A value of true means hide the parameter from the user, the default attribute will be used for the value.	No
Optional	A value of true and the user isn't required to supply a value.	No
Category	This integer value determines how the parameter is grouped. Parameters of the same category will all be grouped together.	No

The <tunnel> Element

This element sets up a secure TCP tunnel for the application that will forward all data over the secure SSL Explorer link to the hostname and port specified in the "hostname" and "port" attributes. In our VNC example, the hostname and port are set using these parameters and the tunnel is given a name of "VNC".

```
<tunnel name="vnc" hostname="${shortcut:hostname}"
port="${shortcut:port}" usePreferredPort="false"/>
```

There are no restrictions on the number of tunnels that can be configured for a single application, but each tunnel must have a unique name. The name given to the tunnel is important because you also need to be able to configure your application's command line to connect to the tunnel created by the VPN client. The VPN client will automatically select a random port and create a pair of parameters to allow you to reference the selected port and listening address. It does this by using the tunnel name to dereference the parameter.

Attribute	What it Means	Required?
Name	A unique name for the tunnel e.g. "vnc".	Yes
Hostname	The hostname of the destination host. This value is referenced by using a string replacement variable to substitute the entered hostname.	Yes
Port	The port to connect to on the destination host.	Yes
usePreferred Port	If this value is set to 'false' then the VPN client won't try and open tunnels on the preferred port, it will just open a random port straight away.	No

Type Elements

Depending on the application type (Java, executable or HTML), different 'Type Elements' will be required.

1. Java

For the deployment of Java applications, use the "Java" type element. One attribute is required, 'jre' that specifies the minimum Java runtime version required to run the application.

All Java applications must have a class path. This is a collection of files and directories that contain the Java byte code files that contain the applications instructions. Currently we only support the use of *.jar files so any applications that contain directories of *.class files must be packaged into a jar before they can be used.

In our example VNC application file we have simply placed a <jar> element in which the contents contain the path of the jar file relative to the *application.xml* file. You add as many <jar> entries as you like and there are attributes that control whether the file is actually included in the class path.

The 'main' element instructs the VPN Client on how to launch the Java application. You can add as many arguments as required. Each single argument should be enclosed within an <arg> element. If you have JVM-specific arguments, such as the setting of a system property, use the <jvm> element but DO NOT include '–D' or "/d" as this is added by the VPN client according to the Java Runtime Environment installed

For example:

```
<java jre="1.1">
      <classpath>
        <jar>VncViewer.jar</jar>
      </classpath>

   <main class="VncViewer">
        <arg>HOST</arg>
        <arg>${tunnel:vnc.hostname}</arg>
        <arg>PORT</arg>
        <arg>${tunnel:vnc.port}</arg>
        <jvm>com.mysystem.property=true</jvm>
   </main>
</java>
```

The Java <files> Element

If your application contains any files that are not part of the Java class path, you can add them using this element. As with the <classpath> element, the content of the <file> element is a path relative to the location of the *application.xml* file.

```
<files>
      <file>license.dat</file>
      <file>video.mpeg</file>
</files>
```

2. Executable

This type element for native application execution requires one attribute 'program' that specifies the native program to launch. This application's location must currently be on the PATH.

All the child elements are used for the arguments in the same way as the 'java' type. For example,

```
<executable program="mstsc.exe">
      <if parameter="fullScreen" value="true">
         <arg>/f</arg>
      </if>
      <arg>/v:${tunnel:rdp.hostname}:${tunnel:rdp.port}
      /w:${param:width} /h:${param:height}</arg>
</executable>
```

3. HTML

This requires on type element 'html' that has one required attribute 'template' that specifies what the filename of the template page is (see section 'HTML Templates'), and one option attribute 'window' that is passed on to the popup window that contains the applet and is used to define window size and other browser options. For example:

```
<html window="left=20, top=20, width=620, height=420,
defaultStatus=0, status=0, toolbar=0, resizable=1,
menubar=0, scrollbars=0" template="template.html"/>
```

String Replacement

String replacements are used in both *application.xml* files and the HTML templates for the 'html' application type. The table below is a list of all available tokens that you may insert into your *application.xml* file that will be replaced at runtime by SSL-Explorer with actual values.

They take the format:

```
${<category>:<key>}
```

Note: All old format %NAME% variables have been replaced with this format.

String replacements occur in three different places, and the replacements available vary between these. This is best illustrated in a table (one per category).

The Server, Client and HTML columns denote where the replacements will occur:

- **Server** – The replacement will occur during initial processing of the application descriptor.
- **Client** – The replacement will occur at the client end after the application.xml has been downloaded but before the application is launched.
- **HTML** – The replacement will occur on the template when it requested.

property

Name	Description	Server	Client	HTML
<*propertyName*>	Replaces with an arbitrary SSL Explorer system property	✓		✓

request

Name	Description	Server	Client	HTML
serverName	Replaces with the host name of SSL Explorer as the client sees it.	✓		✓
serverPort	Replaces with the port that SSL Explorer is running on as the client sees it.	✓		✓
param.<*name*>	Replaces with an arbitrary HTTP request parameter.	✓		✓

session

Name	Description	Server	Client	HTML
username	Replaces with the username for the currently logged on user.	✓		✓
password	Replaces with the password for the currently logged on user.	✓		✓

shortcut

Name	Description	Server	Client	HTML

<*parameterName*>	Replaces with an arbitrary application shortcut parameter (as defined in the application.xml)	✓		✓

application

Name	Description	Server	Client	HTML
id	Replaces with the ID of the application being processed	✓		✓
name	Replaces with the name of the application being processed	✓		✓
description	Replaces with the description of the application being processed.	✓		✓
path	Replaces with the base path of the application store, i.e. /fs/apps/<id>.	✓		✓

ticket

Name	Description	Server	Client	HTML
id	Generates a new pending VPN session ticket for use by an application that supports the embedded client.	✓		✓

sslexplorer

Name	Description	Server	Client	HTML
host	The hostname on which SSL Explorer is running as it is seen by the client.		✓	✓
port	The port on which SSL Explorer is running as it is seen by the client.		✓	✓
protocol	The protocol on which SSL Explore is running as it is seen by the client (this will be http or https)		✓	✓

tunnel

Name	Description	Server	Client	HTML
<*name*>.hostname	The hostname to which the tunnel is connected. <name> is the tunnel name as defined in the application.xml.		✓	✓
<*name*>.port	The port to which the tunnel is connected. <name> is the tunnel name as defined in the application.xml.		✓	✓

client

Name	Description	Server	Client	HTML
installDir	The directory on the client where the application will be installed.		✓	
localProxyURL	The URL of the clients local HTTP / HTTPS proxy server.		✓	

param

Name	Description	Server	Client	HTML
<*name*>	Replaces with the value of an arbitrary shortcut parameter.		✓	✓

Chapter 10

Frequently Asked Questions

Check here first before submitting support enquiries

ICON KEY
🗀 Valuable information
✎ Test your knowledge
💻 Keyboard exercise
📖 Workbook review

Where can I get support for SSL-Explorer?

Please don't email our company directly for support on this product. We get enough email as it is. You'll be able to seek answers through the SourceForge forum/mailing list at http://sourceforge.net/projects/sslexplorer. For companies interested in support with guaranteed response times, we'll shortly be publishing details of our SSL-Explorer subscription service. There is also now a Knowledge Base available on our website at http://3sp.com/kb where you might be able to find some answers to common problems.

I think I've found a bug, what should I do?

Check out the SourceForge forums detailed above and post as much detail about the circumstances that caused the problem. We need to know your operating system, SSL-Explorer version, Java virtual machine version/manufacturer, **and most importantly, the debug log files generated by SSL-Explorer. Without logging information there is very little we can do to help.**

I'm getting an error code of 1067 when I start the SSL-Explorer Windows service?

Something on your system has port 443 in use. On Windows the likely culprit is IIS. You'll need to stop/disable the IIS service to start.

How do I generate debug information from SSL-Explorer?

Set SSL-Explorer to debug mode from the configuration screen under the SSL-Explorer Home tab.

1) Open the file log4.properties in [install-dir]/conf.

2) Insert the following at the top of the file (if you don't already have this):

```
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=%d{HH:mm:ss}     %-5p
%c{1} - %m%n
```

3) Change the line that says ...

```
log4.rootCategory=INFO,logfile
```

to:

```
log4.rootCategory=DEBUG,logfile,stdout
```

4) Now save the file and open the system.properties file in the same directory

5) Change the line that says:

```
#jcifs.util.loglevel=3
```

to:

```
jcifs.util.loglevel=3
```

6) Restart SSL Explorer and perform the steps you take to reproduce the problem.

These log files are going to be pretty large, so can you email both sslexplorer.log and wrapper.log to support@3sp.com. Please include a link to this post in your message. Any replies will be posted back to this forum.

Can I use FTP over SSL-Explorer?

As of the 0.1.7 release, there is no support for the forwarding of FTP connections. This will require modifications to the operation of the VPN client. We are aware that this is a common request and we'll keep you informed of progress on this one.

What about support for client/server side digital certificates?

We're aware that the authentication processes could be made stronger for the more security conscious amongst you. Enterprise-grade security is out of the remit of the GPL product but we will soon be bringing to market a commercial module for those organizations where strong multi-factor authentication is a fundamental part of their security policy.

Are you going to develop a network connect feature for a true IPSec VPN replacement?

Yes. ☺